Modelling Digital Banking Attackers – Attacker-Centric Approaches in Security

Caroline Moeckel

Thesis submitted to the University of London
for the degree of Doctor of Philosophy

Information Security Group

School of Engineering, Physical and Mathematical Sciences
Royal Holloway, University of London

2020

Declaration

I, Caroline Moeckel, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated. This thesis has been generated by me as the result of my own original research, whilst enrolled in the Department of Information Security at Royal Holloway, University of London, as a candidate for the degree of Doctor of Philosophy. This work has not been submitted for any other degree or award in any other university or educational establishment.

Caroline Moeckel, August 2020

Abstract

While 'thinking like an attacker' is a perspective commonly put forward in security, the usefulness and value of focussing on attackers when thinking about threats is contested in the security community, especially in the area of threat modelling. Using the case example of digital banking, this thesis aims to examine and discuss attacker-centric approaches and thinking in security: both at a high-level to evaluate the views of security professionals regarding such methods, but also specifically focussing on key examples of attacker-centric tools such as attacker categorisations and personas.

The intent behind this work is therefore two-fold: firstly, an enquiry into attacker-centric security thinking and its methods; and secondly, a detailed analysis of attacker-related data, resulting in a presentation of key characteristics and behaviours of digital banking attackers. To realise this, a dataset of over 300 items of open source information on cases of cybercrime against digital banking systems is analysed using grounded theory, identifying factors such as personal traits, group structures and geography as well as modus operandi, targets and legal implications.

Building on these results, an attacker typology containing seven attacker types is proposed, including a heuristic evaluation. Forming the second study within this thesis, a construction method borrowed from user-centred design is adopted to build a set of seven realistic, but fictional, attacker personas. An enquiry into the perception of these attacker personas using a survey study amongst 85 financial services practitioners is completed for validation purposes. A third study examines the role of attacker-centric approaches and thinking in security through 12 in-depth interviews with senior financial services practitioners.

Several original contributions can be identified for this thesis. An overview on malicious users (attackers) in a specific business context is provided, including a detailed investigation into the nature of digital banking attackers grounded in real-life data. Existing socio-technical methods are evaluated and extended using these initial findings, producing tangible and data-driven outputs in the form of an attacker typology and attacker personas specific to digital banking. A unique focus on attacker-centric security thinking in theory and practice is offered, providing guidance on how such approaches may be used in both academic research and security practice in the future.

Acknowledgements

This PhD research has seen no less than four house moves, three new job roles, a dog, one wedding, one funeral and also the birth of our daughter Nina. While it has been a difficult journey at times, I have certainly learned more than I could have ever imagined.

I would like to very much thank Dr. Geraint Price for his seemingly endless patience as a supervisor of this project at Royal Holloway. I also would like to thank Dr. Rikke Bjerg Jensen at Royal Holloway and Prof. Debi Ashenden at the University of Portsmouth as examiners of this thesis for some valuable feedback that ultimately made this a better thesis. Many thanks to Dr. Konstantinos Mersinas at Royal Holloway for reading and commenting on my drafts. Also to Prof. Sissi Closs at the Hochschule Karlsruhe for taking me under her wing towards the end of this thesis as a mentor. Lastly, thanks to Prof. Ali E. Abdallah at Birmingham City University and Xristine Faulkner at London South Bank University for giving me the confidence to embark on this journey in the first place.

I would also like to thank all my colleagues at the German and UK financial services institutions I have worked with over the years for supporting me (or at least asking the right questions) somewhere along the way through my studies. It has also been great to hear from two people whose work and books have inspired me a lot throughout this research: Adam Shostack and his writings on threat modelling as well as Dr. Lene Nielsen and her work on personas in user-centred design. Thanks also to the excellent group of people I shared the office at McCrea with at some point or other — I am looking forward to hearing more about your future adventures in academia and beyond.

Thanks to my family for always providing me with the opportunity to do what I wanted in life — it means a lot to me. Lastly, I don't think I can ever thank Simon Dover enough for the many words of sanity and encouragement over the years — you have truly been amazing.

Contents

List of Figures

List of Tables

Publications

This thesis is partly based on the following publications:

- C. Moeckel, "Attacker-Centric Thinking in Security — Perspectives from Financial Services Practitioners" in *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES'20)*. Virtual Event. ACM.

- C. Moeckel, "(De-)Constructing Attacker Categorisations: A Typology Iteration for the Case of Digital Banking" in *Journal of Universal Computer Science (J.UCS) Special Issue on Information Security Methodology, Replication Studies and Information Security Education*, vol.26. Accepted/in print.

- C. Moeckel, "Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking," in *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES'19), 1st International Workshop on Information Security Methodology and Replication Studies (IWSMR'19)*. Canterbury, United Kingdom. ACM.

- C. Moeckel, "Researching Sensitive HCI Aspects in Information Security: Experiences from Financial Services (position paper)," in *Sensitive Research, Practice, and Design in HCI Workshop: ACM CHI Conference on Human Factors in Computing Systems (CHI'19)*. Glasgow, United Kingdom.

- C. Moeckel, "From User-Centred Design to Security: Building Attacker Personas for Digital Banking," in *Proceedings of the 10th Nordic Conference on Human-Computer Interaction (NordiCHI'18)*. Extended Abstract. Oslo, Norway. ACM.

- C. Moeckel, "Building Attacker Personas in Practice — a Digital Banking Example," in *Proceedings of the 32nd British Human-Computer Interaction Conference (BCS HCI'18)*. Belfast, United Kingdom. ACM.

Abbreviations

AI	Artificial Intelligence
ATM	Automated Teller Machine
BCS	British Computer Society
CAPEC	Common Attack Pattern Enumeration & Classification
DDoS	Distributed Denial of Service (attack)
DFD	Data Flow Diagram
EMV	Europay, Mastercard and Visa
EU	European Union
FCA	Financial Conduct Authority (UK)
GDPR	EU General Data Protection Regulation
HCI	Human-Computer Interaction
IoT	Internet of Things
IP	Internet Protocol (address)
IS	Information Security
IT	Information Technology
ML	Machine Learning
NCA	National Crime Agency (UK)
NCSC	National Cyber Security Centre (UK)
OWASP	Open Web Application Security Project
PASTA	Process for Attack Simulation and Threat Analysis
PIN	Personal Identification Number
Ref/Refs.	Reference/References
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TAN	Transaction Authentication Number
UK	United Kingdom of Great Britain & Northern Ireland
US	United States of America
UX	User Experience
VERIS	Vocabulary for Event Recording and Incident Sharing
VPN	Virtual Private Network

Part I

Research Context

"Security problems don't exist without an adversary" — follows the logic that an existent vulnerability which is not exploited by an attacker will not lead to an attack and hence a security problem.

— Virgil D. Gligor,
Carnegie Mellon University [1]

1 Introduction

This chapter provides an introduction to this thesis, defining the underlying motivation that has encouraged this research. It sets out the main research aims and objectives as well as related questions and expected contributions. Finally, the structure of the thesis is set out to help guide the reader.

Real-world systems such as digital banking applications continuously face a range of threats. Threat modelling as introduced and further described in Howard & LeBlanc in the context of their work on writing secure code in [2] can help to identify, conceptualise and present these threats as well as related vulnerabilities for a given system and business case. Various frameworks and methods have been developed in support of threat modelling as a security discipline, both in the academic and commercial space: e.g. the STRIDE[1] mnemonic proposed by Microsoft. Here, different approaches will use different foci to inform the underlying structure and offer guidance for building the threat model: they can be understood to be either asset-/risk-, software-/system-centric or lastly, attacker-centric [4][5][6]; depending on what they are aiming to model and identify threats against.

[1]Introduced as part of threat modelling procedures within Microsoft's Security Development Lifecycle as outlined in [3], the STRIDE mnemonic represents six types of threats (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege) that can be used to identify threats to a system once it has been theoretically decomposed, for example using data flow diagrams (see also example on p.26).

While threat modelling methods currently in existence[2] use various foci and levels of formalisation, taking an attacker-centric approach seems contested in literature. Over the last decade, Adam Shostack as a central figure in threat modelling and author of several key works in the field[3] has been a strong advocate against approaches requiring security professionals, developers and other stakeholders to 'think like an attacker'; stating that most security professionals will not be able to effectively and efficiently threat model based on a relatively unstructured list of attackers or by simulating how a mostly unknown attacker is likely to think or act (potentially also introducing own bias [5][7][6] p.41). Other academic works in the area of threat modelling (e.g. Martins et al. [8], Meland et al. [9], Moeckel [10], Palanivel & Selvadurai [11], Potteiger et al. [12] and Surridge et al. [13]) follow this line of thinking, giving preference to asset-/risk- or system-centric views for their ability to model on existing elements such as data flows or stores.

In contrast, Mead et al. saw encouraging results for attacker-centric methodologies in their evaluation efforts [14] using attacker-centric 'persona non grata' representations of "archetypal users who behave in unwanted, possibly nefarious ways". The positive value of attacker-centric threat modelling is also recognised by others, e.g. Kayem et al. [15] in their comparative analysis of threat modelling approaches, the works of Munaiah et al. [16] around attacker mindset or examples of new attacker-centric threat modelling frameworks such as Johnson et al. using attack graphs [17]. 'Thinking like an attacker' has also seen wide uptake in the professional security community (e.g. [18]), with attacker-centric thinking also forming part of university courses [19][20].

However, many approaches to threat modelling, whether formal or informal, flex between different foci and perspectives, with e.g. Mead et al. suggesting combining system- and attacker-centric modelling into a hybrid approach in [14] and Atzeni et al. calling on attacker personas to prevent potential modeller bias encountered in other methods (e.g. attack trees) in [7]. Deriving from user stories in agile software development, Hurlbut describes the usage of attacker-based stories to support system-centric threat modelling in a commercial context [21]. And despite his issues with attacker-centric threat modelling, Shostack includes attacker lists and personas as examples of attacker-centric tools as appendices in his book [6].

Specific attacker-centric tools and techniques range from relatively simple (e.g. Barnard's list in [6] p.478) to more complex attacker lists (e.g. Intel Threat Agent Library [22]), also including more detailed attacker categorisations (e.g. attacker taxonomies [23][24] and typologies [25][26]) and attacker personas as human-like representations of attackers (e.g. in [7][27]). However, these approaches are not without methodological issues: Atzeni et al. [7] identify a lack of grounding in real data for attacker personas, while De Bruijne et al. [26] criticise the limited provision of procedural and methodological detail in previous attacker categorisation efforts. This is in strong contrast to the relative maturity of traditional persona creation methods in user-centred design, with dedicated textbooks and structured process models available (e.g. *The Essential Persona Lifecycle* by Adlin & Pruitt [28] or

[2] A helpful overview of the 12 major threat modelling methods is provided by the Software Engineering Institute at Carnegie Mellon University in [4]; see also Section 2.2.

[3] His works include one of the few books solely dedicated to threat modelling: *Threat modeling: Designing for security* [6] and the regularly cited paper *Experiences Threat Modeling at Microsoft* [5].

Nielsen's 10 step process for building personas in [29][30]). Similarly, attacker categorisations have only made limited use of theoretical building blocks dedicated to typology or taxonomy building processes, including the distinction between these two terms (e.g. in Seebruck [25]) or heuristic evaluation efforts (suggested in [26]).

This thesis aims to address several aspects surrounding the debate around attacker-centric approaches in security and the indicated limitations, both at a high-level to evaluate the views of security professionals regarding such methods, but also specifically focussing on key examples of attacker-centric tools such as attacker categorisations and personas.

To accommodate this, an example community of attackers is analysed to help build a new attacker typology and set of attacker personas. Here, digital banking[4] has been selected as a sector case study to focus this research, using a dataset of over 300 publicly available documents mentioning digital banking attackers and their characteristics as a basis for analysis. In direct alignment, professionals in financial services (specifically in the areas of security, risk and fraud) have been invited to provide their perspectives on attacker personas specifically, but also on the wider context of attacker-centric security elements in their everyday routines.

Digital banking case studies are not new in an academic context, both related to threat modelling [10][31], but also in a more general socio-technical context. Examples include cross-cultural comparison efforts examining customer adoption of mobile banking in [32], or specific technical security problems, e.g. the detailed examination of a previously undetected vulnerability affecting the EMV protocol for card payments ('chip and PIN') from 2014 in [33]. Beyond offering a wide range of interesting research angles at the intersection of security, usability and business requirements, also involving a number of stakeholders such as users, banking and security professionals as well as attackers, certain practical benefits can be expected from choosing this focus area. Firstly, examples of digital banking cybercrime seem widely available (e.g. as part of various databases collecting such information like the Cambridge Computer Crime Database [34] or in [35][36][37]) — although dedicated attacker categorisations limited to digital banking were not found by the researcher at the time of finishing this research project. Secondly and specific to this research, the affiliation of the researcher with two European banking organisations over the course of this research was seen as beneficial for gaining insights and access to a network of banking professionals working across security, risk and fraud functions.

As reflected in the title of this thesis, the intent behind this work can therefore be understood as two-fold: firstly, the focus of this work is on the enquiry into attacker-centric security thinking and its methods (such as attacker categorisations and personas), also considering the perspective taken by financial services practitioners in this context. The second intent of this research can be described as a detailed analysis of attacker-related case data, resulting in a baseline overview of key characteristics and behaviours of digital banking attackers.

[4]In this thesis, digital banking (as defined in Section 2.5.1) is understood as the integration of digital technologies into the overall banking business model and organisation along the entire value chain and in all areas of financial services provision, ranging from e.g. personal or business banking products, transactional services, financing or investment offerings, but also in areas such as human resources, marketing and customer services. Examples may include mobile banking apps, interactive chat bots for customer support or online trading facilities.

Following this introduction, this chapter is organised as follows: initially, the principle aspects motivating this thesis are set out. Derived from this, the main research aims and objectives as well as questions and further subordinate questions guiding the research are stated, followed by a note on expected contributions. Lastly, the structure of this thesis (including an overview of all parts and chapters) is explained as a guide to the reader.

1.1 Motivation

The following aspects and problem fields have motivated the research carried out and included in this thesis:

- *Diverging views on the value and usefulness of attacker-centric approaches* — as indicated in the introduction, views in both academia and a professional context regarding research approaches, tools and techniques with a primary attacker focus seem to be diverging. While threat modelling methods focus on assets or system elements to provide a structure to model against, generally dismissing an attacker-centric focus, this seems at odds with thinking around security inspired by the underlying premise of 'thinking like an attacker' and existence of dedicated attacker-centric tools like attacker lists or personas. This opens up routes of enquiry into real-world usage of such approaches including potential issues and shortcomings as well as future potential.
- *Professional perception and practical uptake of such approaches* — in direct relation to the last point, security practitioners will likely hold their own mental models[5] of systems and how attackers may have an impact on them [38][39]. While partially informed by current data and learnings constructed within their organisation, past personal experiences, beliefs and background (e.g. education and skillset) will influence the view they take on human attackers, including all biases and assumptions brought forward by the individual (e.g. mentioned in Atzeni et al. [7] and Shostack [6] p.41 in the context of attacker personas and lists). Whether intentionally or subconsciously, practitioners working in the fields of security, fraud or risk can be expected to rely on approaches, tools and techniques and ways of thinking that are attacker-centric at least to some degree, with varying levels of structure and formality. Research efforts to inspire and draw upon for enquiries into work routines involving attacker-centric elements as well as the perception of such approaches can for example be found in the HCI and UX space: e.g. Bruun et al. [40] interviewed 10 UX professionals to explore their role in agile development, while Bodker et al. reviewed the level of acceptance and effectiveness for (user) personas in a real-world project setting in [41].
- *Methodological inconsistencies around attacker categorisations as an attacker-centric method* — as a specific attacker-centric approach and tool, structured attacker lists such

[5] In their primer on mental models in human-centred security, Volkamer & Renaud choose the definition by Rouse & Morris for its generic nature, able "to encapsulate the meaning of all the different terminologies" identified in their literature review — mental models can therefore be understood as "mechanisms whereby humans generate descriptions of system purpose and form, explanations of system functioning and systems states, and predictions of future system states" [38] p.257.

as typologies and taxonomies can provide interesting and accessible representations and visualisations of human threat actor landscapes, but may suffer from methodological limitations and shortcomings at this point in time. De Bruijne et al. conclude on "a disheartening picture of state-of-the-art thinking on threat actor typologies" in [26], citing a number of issues such as lack of transparency regarding underlying data sources as well as employed classification and construction methods. Additionally, a number of key categorisation efforts seem to build on each other, referencing previous literature rather than introducing independent real-world datasets (e.g. [24][25][42]), with one of the key references in the area (Rogers [43]) not meeting certain standards (such as clear publication date and route, named data sources and methodology).

- *Transition of attacker personas from academic theory into business practice* — another specific attacker-centric approach and tool, attacker personas and their creation methods have been introduced and described largely in an academic context. Here, Steele & Jia initially proposed anti-personas, -scenarios and -use cases to embody archetypical attacker characteristics and behaviours in [44]. This was further formalised in Atzeni et al. describing their methodology for attacker persona creation in [7]. While these works, as well as other key publications on the topic of attacker personas such as Faily & Fléchais [27] or Tariq [45], provide examples of attacker personas or their application in organisations in the form of case studies, no full attacker persona set or related narrative stories are presented within the often limited scope of conference papers or journal articles. Furthermore, detailed enquiries into the practical acceptance and use of attacker personas by professionals in organisations in line with user personas in HCI research [30][40][41] seem limited at this point in time.
- *Application of digital banking as a sector-specific case example to the field of human-centred security/HCI for security research* — lastly, research into attacker-centric approaches specific to applied business cases or specific sectors (such as digital banking in this thesis) seems to be limited to date, with e.g. attacker categorisations efforts [23][25][42][46] remaining at a generic level (although attacker persona studies have focussed on specific case studies in the past, e.g. a multi-device open-source platform in [7] or rail infrastructures in [47]). As an accessible, interesting and multi-faceted applied case example, digital banking can be seen as a highly user-centric, experience-driven business model that balances usability and security for a very large user base in an everyday context. It has therefore found relatively widespread entry as an area of application in threat modelling as well as usable security literature in the past (e.g. in [31][48][49] and [50][51][52] respectively), also in previous works in these areas by the researcher [10][53].

1.2 Research aims

Based on the introduction and motivation, the following high-level aim and subsidiary aims can be stated as the purpose and statement of intent for this thesis. This is followed by research objectives in the next section, further indicating the procedural steps to help achieve these goals, before presenting the research questions to be answered in direct support of this.

The primary aim of this thesis is to explore and clarify the role of attacker-centric approaches in security within the real-world context of digital banking and subsequently apply it to two existing key attacker-centric methods: attacker categorisations and personas. **As a first subsidiary goal,** a fundamental enquiry into the nature of attackers targeting digital banking services based on an analysis of related cybercrime cases is attempted, both to support the practical research work carried out in this thesis, but also as an independent, referable research outcome. **As a second subsidiary goal,** suggestions for guidance on usage of attacker-centric security approaches, related methods and tools are sought to be established, also in collaboration with security, risk and fraud practitioners working in financial services.

This work is intended to directly complement and link in with previous research in the following ways: firstly, in the area of threat modelling, further clarity around how practitioners employ an attacker focus in their daily practice may help to align attacker-centric ways of thinking with existing formal and informal approaches. Secondly, issues apparent in previous attacker categorisation works (for example lack of methodological transparency, also regarding underlying data sources as raised in De Bruijne et al. [26]), are addressed by stepping through an attacker categorisation exercise using the example of digital banking. Thirdly, for the area of attacker personas, works such as Atzeni et al. [7] and Faily & Fléchais [27] are complemented by providing a full visualisation and documentation of an attacker persona set including narrative stories (in contrast to examples limited to individual personas only).

1.3 Research objectives

Further to these overall research aims, a number of research objectives to be achieved within this thesis (at least partially) can be stated.

Research Objective 1 —
Provide a detailed, but focussed enquiry into the state of research surrounding attacker-centric security approaches, related methods and tools by undertaking and documenting a literature review of commercial and academic materials.

Research Objective 2 —
Define a dedicated set of methods to serve as a comprehensive research design framework for this research project, by addressing gaps and inconsistencies in related literature, but also building on methods applied in previous works and drawing on insights from other disciplines such as HCI or UX design.

Research Objective 3 —
Establish a comprehensive picture of attackers targeting digital banking services, their characteristics and behaviours through data analysis of real-world data samples to enable an informed enquiry into attacker-centric security in this area; firstly, as an initial foundation for further research activities, but also as a tangible deliverable in itself.

Research Objective 4 —

Extend the analysis of real-world digital banking attacker data by identifying traits shared by attackers with the aim of constructing an attacker categorisation specific to digital banking, also linking back to previous research in this area and to include evaluation efforts.

Research Objective 5 —

Develop a set of attacker personas specific to digital banking building on the insights previously gathered on attackers in this area and directly extending the attacker categorisation, also linking back to previous research in this area and to include evaluation efforts.

Research Objective 6 —

Further explore the state of attacker-centric security, methods and tools in practice, specifically for digital banking and financial services, by working with practitioners in this field and collecting, analysing and structuring their opinions and thoughts on this subject. Additionally, synthesise these insights into suggestions for guidance and recommendations on the usage of such approaches in practice.

1.4 Research questions

To help achieve the research aims and objectives set out, the following five high level research questions, supported by a number of related subordinate questions, can be formulated.

Building on the first two research objectives, the first research question addresses the theoretical grounding behind attacker-centric security as well as related tools and methods, underpinning some of the debates motivating this thesis as indicated in the last sections.

Research Question 1 —

What role does an attacker focus and usage of attacker information play in security literature?

- Further to this, how can attacker-centric security be defined based on previous literature?
- Which specific approaches, tools and methods can be identified from literature in this context?
- Which usage scenarios, direct value and benefits can be observed for such approaches?
- Similarly, which limitations have been raised in this context?
- If any, have proposals for future usage of attacker-centric approaches been made?
- Lastly, for the specific setting of digital banking, how (if at all) has an attacker focus be used in this context to date? Which examples of attacker-centric security approaches can be found?

To help enable the usage of digital banking as a case example, the second research question demands a detailed investigation into the nature of attackers targeting such systems, also setting the basis for the practical research activities building on this information (as stated in Research Objective 3 and further expanded on in Research Questions 3 and 4).

Research Question 2 —

Which common characteristics and behaviours can be identified for attackers targeting digital banking systems through data analysis?

- Which data sources, available in the public domain and specific to digital banking, can be used to explore the nature of attackers?
- Which methods and procedures can be summarised into a methodology for working with this data, enabling deep engagement and detailed exploration as well as structured analysis and coding around common themes encountered?
- Emerging directly from the data analysis, which criteria can then be identified to describe attackers, their characteristics and behaviours, as well as to help structure the presentation of analysis results?

Focussing on specific attacker-centric tools and methods and using the insights and results gathered through Research Questions 1 and 2 previously, the next set of research questions guides the evaluation, re-framing and application to digital banking for two specific attacker-centric methods: attacker categorisations and persona visualisations, as indicated in the motivations and prepositioned in Research Objectives 4 and 5.

Research Question 3 —

In line with previous research in the area of attacker categorisations, how could a set of attacker types look for the case of digital banking as an example of an attacker-centric method in security?

- Reflecting on previous efforts in this area of research and their respective methods, can a transparent and comprehensive methodology for building an attacker categorisation grounded in data be devised?
- Which criteria are best used to describe these attacker types? Which attacker characteristics and behaviours are best used to inform these criteria?
- From the results of the data analysis in answer to Research Question 2, which clusters of attackers can be identified for this business example?
- How does this set of attacker types differ from general attacker classifications as found in prior attacker taxonomies and typologies?
- Which verification efforts can be recommended and undertaken to confirm the logical structure and fit to data for the new categorisation? Will amendments to the original categorisation be required?

Research Question 4 —

Building directly on the results from the data analysis, how would a complete and detailed set of attacker personas be defined and visualised for the case of digital banking as another example of an attacker-centric method in security?

- In line with previous research in the area of attacker personas and their methods, but also reflecting on methods used for the creation of traditional user personas in an HCI and UX context, how could a structured and data-driven approach for building attacker personas look?
- Extending on the examples shown in previous literature, which blocks of information should be included when aiming to produce a complete, detailed and useful attacker persona set?
- In an evaluation effort, how do security practitioners in financial services perceive the value of attacker personas as an attacker-centric security method, in general and for the specific persona set built in this thesis?
- Lastly, considering the evaluation outcomes, which amendments are indicated? Can guidance on future uses of this method be provided for practitioner use?

Lastly and prepositioned in Research Objective 6, and pulling together insights in answer to the previous research questions, the last research question addresses the overarching theme of the usefulness and value of attacker-centric approaches and thinking in security in practice, focussing specifically on the case of digital banking and financial services.

Research Question 5 —

How are attacker-centric security approaches used in practice and what value do they provide to security practitioners in financial services?

- Which attacker-centric security approaches are security practitioners in financial services aware of and/or use on an everyday basis? Which role do they currently see an attacker focus play in their formal or informal threat modelling activities? And how do they use attacker information and related data in practice?
- Where do they see opportunities to employ attacker-centric thinking? What are the benefits and value they assign to adopting such perspectives?
- Furthermore, which overall limitations or hindrances to using an attacker focus in the first place do they state?
- Lastly, what potential do they see for attacker-centric thinking in the future? In their opinion, should these approaches be used differently going forward, and are emerging security trends or threats likely to influence this?

1.5 Expected contributions

Summarising on the motivation, aims and objectives as well as questions behind this research as stated in this chapter, five original contributions to the current state of knowledge can be envisaged for this thesis.

- *Provision of an initial definition, comprehensive overview and assessment of attacker-centric approaches in security* — incorporating a systematic review of related literature; also taking into account practitioners' views (limited to financial services) on the subject. As a tangible outcome, a list of recommendations and guidance points on using an attacker-centric focus in research and practice is to be provided.
- *Presentation of attacker types applicable to digital banking in the form of a categorisation overview* — replicating previous research efforts (e.g. [23][24][25][42]) for the specific case of digital banking. As a further extension to these works and to address methodological inconsistencies such as lack of transparency regarding underlying data sources (as identified e.g. in De Bruijne [26]), a dedicated reference dataset and categorisation method including evaluation efforts is to be introduced within this thesis.
- *Creation of a set of attacker personas applicable to digital banking* — extending on previous works in this area such as e.g. Atzeni et al. [7] or Faily & Fléchais [27], but with the intention of providing a fully documented attacker persona set, both grounded in data and following user-centred design principles. It is expected that this attacker persona set will be useful for reference purposes for both academic peers and practitioners, with an assessment of the practical value of such methods to be included within this thesis.
- *Provision of a detailed analysis covering characteristics and behaviours of digital banking attackers* — based on a grounded theory method analysing over 300 publicly sourced materials from four different data sources (see Section 3.4.1). While this contribution directly supports the creation of both the attacker categorisation and personas in this work, it would also be expected to be of interest to academic peers and practitioners as a stand-alone research deliverable — however, the data sources used would likely require careful and continuous review and updating to maintain their relevance and validity over time.
- *Provision of a case study for grounded theory usage in a security context* — lastly and as a supplementary contribution, grounded theory as used within the data analysis mentioned in the last point, has found entry into information systems literature in the past (as reviewed in detail by Urquhart et al. in [54]). For the field of security, it is expected that this work may support future research where this method is considered or being used.

1.6 Organisation of this thesis

Addressing the research aims, objectives and questions stated, the work carried out within the context of this thesis is organised into five parts, including a total of 10 chapters as follows:

Part I — Introduction and background
As requested in Research Objective 1 and the related Research Question 1, the first part includes the introduction (Chapter 1), providing the principle motivation behind this research, together with research aims, objectives and questions as well as expected contributions to set the principle context of this thesis.

The background section (Chapter 2) to this work then assesses the state of attacker-centric approaches in security as brought forward in previous literature, also focussing on key methods and tools in this area such as attacker categorisations and personas. Additionally, digital banking as used within this thesis as an applied case example is defined at this point.

Part II — Research design including data sources
Part II (formed of one chapter: Chapter 3) includes a comprehensive overview of all methodological decisions underlying and informing the work carried out within this thesis, addressing Research Objective 2 and the related Research Question 1. Starting with a view on the theoretical lens and conceptual framework employed, an overview of the sequencing of research activities, note on the positionality of the researcher, full details on data sources used throughout the thesis and lastly, the exact research procedures underlying the individual studies within this thesis (Parts III and IV) are provided.

Part III — Analysis: characterising digital banking attackers
In response to Research Objective 3 and the related Research Question 2, Part III documents the fundamental enquiry into the nature of attackers targeting digital banking, using data analysis procedures and sources as set out in the research design in Part II. Chapter 4 describes their personal characteristics, geographical factors as well as community and group attributes, while Chapter 5 shows results in the area of attacker behaviours, including preferred targets and modus operandi as well as legal aspects.

Part IV — Meta-analysis: attacker-centric representations
Part IV is made up of three chapters and builds directly on the results of the analysis presented in Part III. From this, Chapter 6 sets out to describe clusters of attackers in an attacker typology specific to digital banking (in answer to Research Objective 4 and Research Question 3). Further extending on this and also incorporating the results from Chapter 4 and 5, Chapter 7 then attempts to create an attacker persona set applicable to digital banking (in answer to Research Objective 5 and Research Question 4).

The last section of this part (Chapter 8) then explores the usage of attacker-centric approaches in security in a practical context, integrating the perspectives of financial services practitioners (in answer to Research Objective 6 and Research Question 5). While this last chapter directly benefits from previous learnings from Chapters 4 to 7, it also conceptually 'opens out' the discussion towards the end of this thesis, with the aim of connecting theory and practice, providing guidance and inspiring future research on attacker-centric approaches in security.

Part V — Future work and conclusion

The last part of this thesis includes two chapters: Chapter 9 is dedicated to suggested future work stemming from the results in this thesis, while Chapter 10 presents a reflection and conclusion, also referring back to the expected contributions listed in this chapter in Section 1.5.

Appendices

Several materials in support of this research are included in the appendix. For Part III, an inventory of all original sources used in the analysis has been included. For Part IV, three items have been included: for Chapter 7, seven narrative scenarios expanding on the attacker personas and a participant information sheet for the survey study with financial services practitioners have been included. For Chapter 8, a participant information sheet for the in-depth interviews with financial services practitioners has been included.

I've spoken for over a decade against 'think like an attacker' and the trap of starting to threat model with a list of attackers.

— Adam Shostack, 2019 [55]

2 Background

Deriving from the research aims, objectives and questions set out in the introduction and preparing for the analysis and studies in the remainder of this thesis, this chapter provides further background and references to previous literature. It is conceptually divided into two parts: the first part starts by assessing attacker-centric perspectives in general, before narrowing its focus on attacker-centric threat modelling as well as attacker-centric approaches such as attacker categorisations and personas. In the shorter second part, digital banking as a case study context is considered, including a basic definition.

To date, the term 'attacker-centric' seems to have been predominantly used in the context of threat modelling, signifying an attacker focussed threat modelling approach in contrast to asset-/risk- or software-/system-centric threat modelling approaches (e.g. in Shostack [6], Surridge et al. [13] or Wills [56]). But attacker-specific aspects are naturally present in the wider context of security research — a variety of approaches will include adversarial elements at various stages of the security process, with varying degrees of abstraction and focus. These may range from abstract representations of malicious users in literature like the adversary in the formal Dolev-Yao model [57] to informal thinking about attackers in every day security practice (e.g. brainstorming sessions in multidisciplinary teams in Shull & Mead [58]). They also include dedicated, attacker-centric approaches beyond threat modelling, like attacker categorisations such as typologies or taxonomies (e.g. the works of Ivoce [59], Rogers [23],

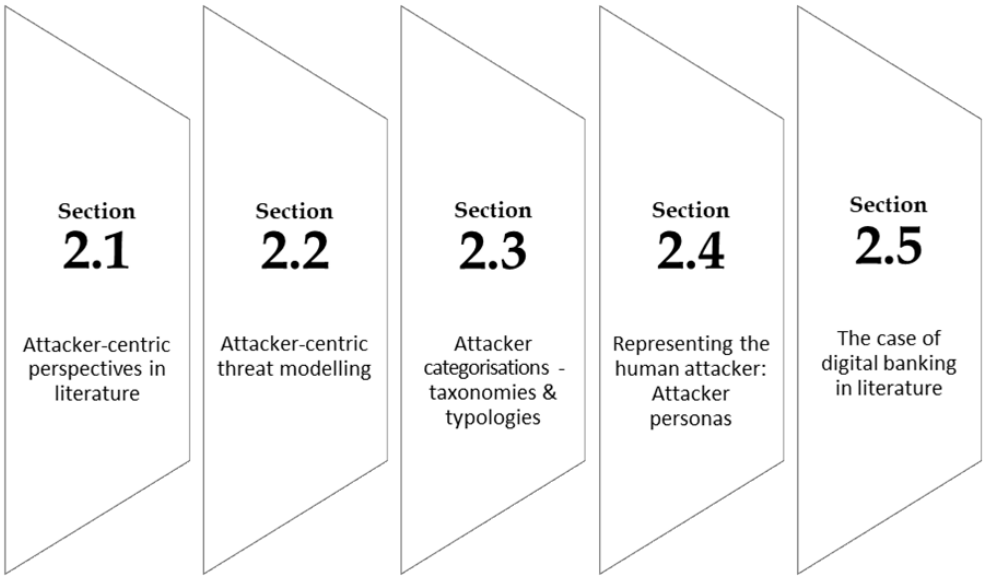


Figure 2.1: ***Elements of literature review and background to this work***

Meyers et al. [42], Hald & Pedersen [24] or Seebruck [25]) as well as attacker personas (e.g. in research from Atzeni et al. [7], Faily & Fléchais [60], Tariq et al. [45] or Steele & Jia [44]), with established and defined bodies of literature surrounding them.

Directly reflecting the structure of the introduction and related to the stated research aims, objectives and questions, this chapter aims to situate and contextualise this research by providing an overview of previous literature — to achieve this, five distinct themes are discussed as shown in Figure 2.1: initially, a compact systematic literature review is carried out, with the aim of establishing a fundamental understanding of the state of attacker-centric approaches in security as a research field. Next, this broader, high-level view is conceptually narrowed down by theoretically expanding on attacker-centric threat modelling as introduced in the beginning of this thesis. This is then followed by a deeper enquiry into two attacker-centric methods found in previous literature: attacker categorisations (like taxonomies and typologies) and attacker personas. This analysis directly underpins the research studies in Chapters 6 to 8 of this thesis.

The last part of this background section — focussing on digital banking — initially aims to provide a comprehensive definition of the topic and its conceptual positioning between usability and security. This is followed by an perspective on attacker types relevant to digital banking as found in past literature. While this overview underlies the entire thesis with its application to digital banking as a case example, it is particularly relevant to Chapters 4 and 5 of this thesis documenting the grounded theory research into digital banking attacker characteristics and behaviours.

2.1 Perspectives on attacker-centric security in literature

To establish an initial description and definition of attacker-centric approaches in security and the related body of literature, a fundamental literature analysis loosely following the work of Kitchenham et al. on systematic literature reviews in software engineering in [61] was carried

out, also using the recent example of a systematic literature review on threat analysis of software systems by Tuma et al. [62] to help guide this process further. The objective was to produce a literature review that was both broad in nature, but specific to the defined topic as well as replicable, transparent and accessible to others. As a light weight adaptation of [61] and [62], a principle search strategy[6] was used to select a literature sample to be reviewed (see also footnote on p.17), leading to a number of related findings on attacker-centric aspects in security. To aid the readability of this section, these are grouped around seven literature themes, including a definition, observed research activity, types of approaches, their benefits and limitations as well as validation efforts, impact on practitioners and future directions.

Employed definition and understanding of 'attacker-centric'

While Applegate & Stavrou [64] explain 'attacker-centric' simply as the "perspective of an attacker's tools, motivations and objectives", no further comprehensive definitions of 'attacker-centric' were found. And although threat modelling literature explicitly refers to the term as one of the potential foci that may be used (see also Section 2.2), most methodological treatments in this context are satisfied to consider the term as self-explanatory and offer no further explanation (e.g. in [13]). Despite this, an attacker-centric perspective seems to be understood and valued in two ways in previous literature. Firstly, and realising that "the adversarial element is an intrinsic part of the design of secure systems" [7], the attacker is naturally an element to be considered in security environments. Secondly, many studies mention an element of 'think like an attacker' or assuming the role of an attacker through attacker-centric perspectives [45][65][66][67], with several authors also discussing this approach critically (for example Shostack [6] or Padmos [68]; also in Section 2.1).

Similarly, the term 'attacker model' is used in two distinct ways: firstly, it signifies the exemplary adversarial view taken when thinking about or assessing the security of a system, for example the specific attacker in mind when building an attack tree [69][70]. Secondly, they may be a set of threat actors which may attack a given system. Here, Fraunholz et al. [71] for example introduce a generic attacker model consisting of various attacker types, e.g. internal/external or state-sponsored/non-state — this basic principle also underlies concepts such as attacker categorisations or personas (refer to Sections 2.3 and 2.4).

Observed research activity levels

Although the initial search results (derived from the search strategy remarked on in footnote 6) showed a relatively high number of potentially relevant items, the final number of selected

[6]The following databases have been used to identify items to be included in this literature review: ACM Digital (Association for Computing Machinery), IEEE (Institute of Electrical and Electronics Engineers), SAGE, ScienceDirect, Scopus, SpringerLink (including Lecture Notes in Computer Science), Virus Bulletin and Wiley-Blackwell as well as Google Scholar. After several pilot studies and initial searches, the following search terms were decided on: "attacker-centric" (alternatively -centred/-centered; also adversary, threat agent); "threat modelling" AND "attacker"; "attacker model"; "attacker profiling"; "attacker persona/s"; "attacker taxonomy/typology" for a date range over the last 10 years (May 2010 to May 2020). Additionally, a review of the references and bibliographies in the initially selected items was carried out ('reverse snowballing' [63]).

items was relatively small (50). And even within this sample, the number of studies with a truly attacker-centric focus was limited: only a limited number of studies used attackers as their central focus in some form, e.g. Adams & Makramalla [72] propose an attacker-centric gamified approach in the context of security training (similarly in [71][73][74]), while research specific to attacker typologies or representations such as attacker personas may be considered as attacker-centric in nature too. Other works would only use attacker-centric aspects in parts of their research, for example as a comparison to other methods (e.g. Mirembe & Muyeba [75] assessing threat modelling methods) or as part of a larger methodological framework, e.g. by Karpati et al. [70] in their *Hacker Attack Representation Model*. This is in line with results from Tuma et al. [62] in their comprehensive and systematic literature review on threat analysis studies, where 45% of studies were considered as 'attack-centric' — it is likely that even fewer of these studies are primarily focussed on attackers. With this currently moderate level of research activity observed for this potential research 'niche', an introduction to literature using a sample of selected literature[7] in this area seems of value to understand its current state and scope as well as present limitations.

Types of attacker-centric elements and approaches

Threat modelling and risk assessments involving attacker elements can be carried out using a large number of techniques, tools and vehicle, which can be classed as follows:

Attack trees or related approaches — attack trees (or threat trees) are described in a large number of studies in the field (e.g. in [66][69][70][76][77][78]; also in [62]), with Kordy et al. proposing an extension to attack-defence trees incorporating both attackers and mitigations [79]. Attack trees, a term introduced by Schneier in [80] and further formalised in Mauw & Oostdijk [69], can be considered as a "formal, methodical way of describing the security of systems, based on varying attacks. Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes" [80]. A graphical representation using a financial services example in the form of an attack against an ATM produced by Mantel & Probst [81] is shown in Figure 2.2.

Goal-based modelling approaches — goals of attackers, but also goals modelled in requirements engineering in a business or software development context are seen to play a role when assessing threats, e.g. De et al. [82] propose a goal-based threat modelling approach for cloud-based environments, while Meland et al. [9] conclude on an overall positive effect when modelling both threats and goals to a system if used as a foundation of risk assessments.

[7] To arrive at the final selection of 50 items in the sample, materials were excluded from the analysis if they were: not sufficiently focussed on attackers or providing detail on how attacker information is used; very abstract and limited attacker representations without consideration of attacker behaviour and characteristics; and lastly not of sufficient quality and reliability. Items should contain information about the authors, institutions involved, clear research questions and objectives, applicable method and logical research design. Items published in journals or conferences with a rating lower than B (good) in their CORE rating were excluded, while conferences or journals with an undefined rating would go through a further round of investigation against these exclusion criteria. The CORE database is a portal ranking both conferences and journals from the Computing Research and Education Association of Australasia (CORE) and is also used as a quality benchmark by Tuma et al. in their literature analysis example [62].

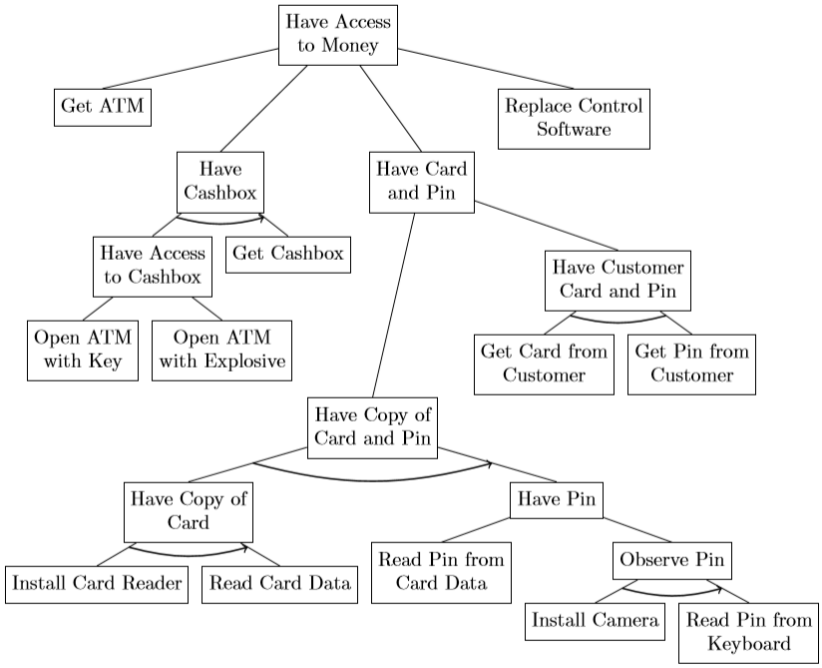


Figure 2.2: ***Attack tree — example attack against an ATM [81]***

Misuse cases and (anti-)scenarios — a number of studies make use of the vehicle of misuse cases, describing potential malicious abuses of a system and the related attacker involvement leading to an exploit or incident. This can take the form of misuse, abuse or anti-use cases [9][44][66][83], misuse maps and diagrams [9][70], anti-scenarios [44][45] or pre-defined attack patterns [66][70] (also in Tuma et al. [62]).

Approaches based on attacker characteristics — attacker characteristics (e.g. skills, resources, intentions or motivations [71]) and behaviours (e.g. in Al-Mohannadi et al. [84], where honeypot experiments are used to gather insights on attacker behaviour) are in the centre of several studies, including attacker representations like attacker personas [7][44][45] or similarly a 'persona non grata' [14][58]: these data-driven, realistic character representations stand in contrast to abstract, formal attacker representations. A theoretical grounding for the subject of attacker personas is provided in Section 2.4.

Attacker lists and categorisations — enumerations of attackers as well as categorisations of attackers, such as taxonomies or typologies of different attacker types and profiles are used in a number of studies to support threat modelling and risk assessment efforts [85][71]. These lists and categorisations may be accompanied by detailed attacker descriptions, including attacker attributes such as intent (hostile/accidental), resource, capabilities and skill level (e.g. Intel Threat Agent Library [74]; also in [78][86]) or group structures and relationships [73]. Extensions such as basic threat or capability ratings may also be employed in this context [71]. A dedicated literature review on attacker categorisations is undertaken in Section 2.3.

Attacker aspects used alongside widely recognised threat modelling elements — while they are not strictly attacker-centric or accommodate formal attacker modelling, representations such as data flow diagrams (DFD), the threat classification mnemonics STRIDE and DREAD (categories for risk assessment: damage, reproducibility, exploitability, affected users and discoverability) as system-/software-centric approaches (as elaborated in Shull et al. [58]

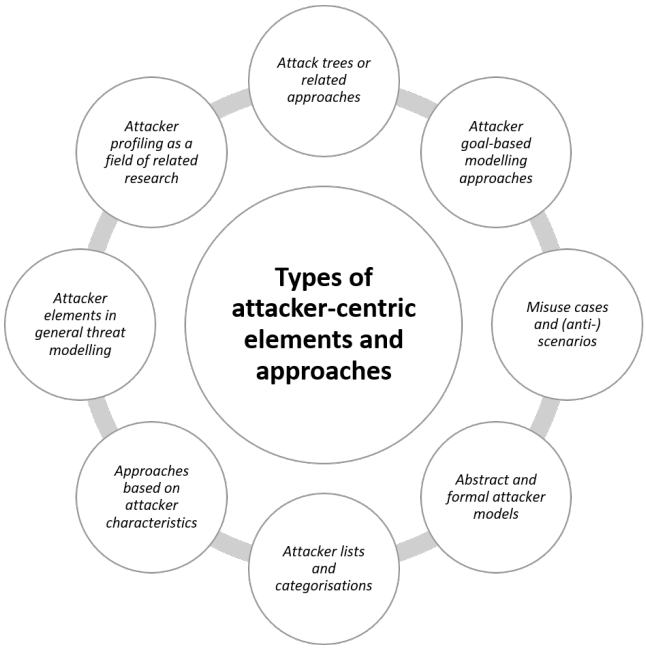


Figure 2.3: ***Attacker-centric elements and approaches identified from literature***

or Shostack [6]) will also consider potential attackers and their actions — this is further elaborated in Section 2.2 on threat modelling specifically.

Abstract and formal attacker models — a well-known formalisation of attackers in the context of security protocol is the intruder within the Dolev-Yao model of security, which dates back to 1983 [57]. Powerful attackers in this model are equipped with a fixed set of capabilities — it is commonly assumed that it will capture any attack initiated by an attacker following the rules of the Dolev-Yao abstraction (further extended to any arbitrary attackers in the proof by Cervesato [57] or "arbitrarily strong attackers" [67]). A range of researchers have expanded and adapted this model to include decision-making and rational behaviour in the form of cost-benefit analysis on the attacker side, leading to 'rational attacker' [87] or 'general attacker' models [88]. Other relatively formal models take a risk-based perspective, including factors such as risk acceptance and skill level to emulate expected attacker behaviour [89] — however, this does not take into account their motivation or other resources. While the focus of this thesis is certainly on less formal approaches, a relatively current overview on adversary models in the context of cryptography has been provided by Do et al. [90].

Attacker profiling as an area of related research — while not directly concerned with the modelling of attackers, but with the aim of gaining a deeper understanding into the exact nature of attackers and cybercriminals, a considerate body of literature can be attributed to the subject of criminal profiling of attackers (or 'hackers'). Researchers working in this area have relied on a variation of blended research designs and data collection methods. As an example of such research efforts, Higgins [91] has used expert interviews to gain an insight into the nature of cybercriminals (without speaking directly to attackers). Leukfeldt [92] for example has used information recorded by the police in interrogations with the attackers, in-depth interviews with case officers and secondary analysis of fraud databases. In their large-scale *Hackers Profiling Project*, Chiesa et al. [93] (ch.4) have outlined gathering data directly from attackers through online surveys, observations at hacking events and honeypot traps

(intentionally vulnerable systems aiming to attract attackers) in their planning. Thackray adds observation ("lurking on forums") as a way of collecting data, together with online surveys and interviews as completed in their research [94]. Yielding unique insights into attack ecosystems, these works may offer valuable support to previously mentioned attacker-centric approaches, both by fostering learning and understanding about attackers, but also as reference points for validation and comparison of abstract attacker representations and models — in this thesis, this benefit is relied on in e.g. ch.4, where reference to e.g. Chiesa et al. [93] is made to compare the findings on digital banking attackers.

Perceived benefits and limitations of attacker-centric approaches

Interestingly, the number of explicitly stated benefits of using an attacker-centric lens is limited in the reviewed literature sample. However, there seems to be an underlying perception that understanding or modelling attackers behind past or potential future attacks is beneficial, e.g. for assessing and subsequently prioritising threats [44], designing and testing countermeasures [74] or forensics purposes [73] or to "provide general insight into the attacker's mind" ([74], similar in [71]). Several authors see the creation of reusable threat agent or attacker reference libraries as useful for future security practice [74][85].

Attacker representations are also considered valuable when interacting with stakeholders: they may support their decision-making and provide confidence in "emergency response situations" [73], but also aid day-to-day communications [70]. Tariq et al. [45] and Yuan et al. [66] also see an attacker-centric perspective as a vehicle of collaboration — enabling and engaging developers, security professionals and other stakeholders to consider illegitimate use cases in product designs, but also to better understand the implications on security caused by their design decisions. In the context of security awareness for employees, Adams & Makramalla suggest the usage of avatars to represent attacker types and their characteristics in their concept proposal for a gamified approach for security skills training in [72].

However, the potential challenge of structuring risk assessments around attackers has been identified across literature. As indicated previously, attacker-centric threat assessments may only provide limited structure to model against, making them strongly dependent on the individual ability, level of training, knowledge and experience of the modeller [13][66][75] — this may also lead to different individuals producing different models, leading to inconsistencies in results [6][77] — the shortcomings of attacker-centric threat modelling specifically are also further analysed in Section 2.2.

While not limited to attacker-centric approaches, several other aspects will likely also affect these methods. Firstly, there seems to be many diverging directions and a seemingly high number of attacker-centric approaches as stated above, which prompts Karpati et al. [70] to suggest that "new modelling methods should be extremely well motivated by [...] limitations of existing methods" (similarly in [9]). Additionally, Tuma et al. [62] also criticise the lack of structured tool support — agreeing to this, Yuan et al. [66] see tool development as a field for future work: here, adequate tool support may help to reduce cost and time spent on security activities. This also raises questions on the overall business integration and adoption of attacker-centric approaches — Ben Othmane et al. [86] for example consider current threat

modelling methods as not effective in allowing prioritisation of threats in relation to business goals and business constraints. Morana & UcedaVelez [77] corroborate this and see processes such as fraud management or incident response as often lacking threat modelling insight, also hinting at an absence of attacker-centric approaches in this context.

From a methodological viewpoint, questions around data sources, abstraction and reusability of models may affect attacker-centric approaches in particular. Rocchetto & Tippenhauer criticise the fact that many attacker models are informally formed 'ad-hoc' rather than from validated, existing sources such as attacker categorisations grounded in data in [85]. Shull & Mead [58] critically discuss the level of abstraction required to help create expressive, yet specific models (also in [75]) — here, attacker-centric models and tools may need careful adjustment to achieve a balance between the level of attacker details and abstraction present. This level of abstraction may also help when reusing attacker-based models: Meland et al. view this as beneficial "for knowledge sharing and to achieve a general increase in efficiency and quality" [9]. Lastly, a lack of measurements for assessing the quality of outcomes for modelling processes is seen as problematic in [62][75], although various validation options can be observed in literature (see below).

Validation efforts for attacker-centric approaches

Validation strategies seem to play an important role in attacker-centric studies and research elements, with only few not providing specific validation efforts to date (e.g. [75]). These do not seem to differ significantly from validation strategies used in general threat modelling: they may include case studies of threat models for a range of applications and sectors, including examples in the areas of e.g. air traffic management [9], connected vehicles and video conferencing [86], drone and IT systems [58] or a threat situation faced by the German Bundestag [71]. Other validation strategies include comparisons to similar approaches in literature [64][71] or exemplary illustrations and demonstrations (without a specific real-world case study, in e.g. [66][69][78][82]). Several authors will use tool support for their validation effort: Meland et al. [95] use the threat modelling tool 'SeaMonster', while Faily et al. [27] use their CAIRIS platform (also in [96]). While none of these approaches seem specific to attackers, other validation strategies have been suggested, including interviews with stakeholders or explorative surveys with subject matter experts [6][45][97] — these human-centred approaches may be particularly suited to assessing the quality of attacker representations when used in organisational settings. From the relative numbers present in the sample and identified by Tuma et al. [62], validation efforts in this context may suffer from an over-reliance on case studies, with limited empirical data collected for dedicated validation purposes.

Implications for practitioners identified in literature

Both benefits and limitations identified will have direct impact on practitioners and their ability to use attacker-centric approaches effectively. Firstly, expectations towards practitioners inherent in attacker-centric approaches may be unrealistic: asking practitioners such as developers and engineers 'to think like an attacker' may prove a challenge to individuals

and not lead to meaningful results [58][86][97]. Ease of adoption and continuous usage may also be hindered by limited tool support and guidelines (discussed in Tuma et al. [62]), while small and medium sized organisations with limited resources in particular may not be in a position to absorb the cost and effort of accommodating attacker-centric methods (or threat modelling exercises in general) [97].

Secondly, practitioners will need to view attacker-centric methods as significantly valuable to them (and all impacted stakeholders) to ultimately adopt, use and benefit from them — crucially, they also have to align with existing security practices and threat modelling methods in the organisation. Shull & Mead [58] see this as a substantial problem, with large differences in approaches observed within or across different organisations and methods used alongside one another without being aligned or integrated adequately in the first place [64][76]. Applegate & Stavrou support this: while previous attacker categorisations are viewed as able to identify technical threats and vulnerabilities by them, they are seen to fall "short when it comes to linking actors with different methodologies, goals and patterns of behaviour" [64]. Related to this, several authors have also highlighted the potential difficulty of making threat modelling processes and its outputs accessible to non-security experts including developers or system engineers (e.g. in [70][97]) — attacker-centric methods in their highly visible nature such as attacker categorisations or personas may be able to counterbalance this effect, although further evidence is required in this context (see also Section 2.3 and 2.4).

Reflection and suggested future directions

As a seemingly heterogeneous field, attacker-centric security varies considerably across a variety of research directions, methods and approaches encountered in related works. One of the most significant observations from the initial review of the literature sample is the wide range of methods with an attacker focus or at least containing an attacker element, ranging from attack trees or misuse case diagrams to formal methods type threat modelling (this is also raised by Meland, Tøndel & Jensen [98]).

Despite this present variation, the overall level of research activity observed in the area can be described as moderate to date, with only a limited amount of 'truly' attacker-centric research studies counted (in contrast to the attacker element playing a partial role, e.g. in the context of attack trees or misuse cases). Where these strict attacker-centric approaches can be observed, they seem tightly interwoven with the area of attacker-centric threat modelling or attacker representations and categorisations like attacker taxonomies and typologies or attacker personas — these areas are therefore further explored in the next sections.

While explicit proposals for future research in the area of attacker-centric security seem limited in the reviewed literature sample, a number of ideas have been brought forward in this context, providing potential starting points for research enquiry in the future:

- further methodological development of existing approaches, ideally enabling further integration and unification with other approaches [12][58][69];
- new methodologies and practices to foster and accommodate collaboration between stakeholders [45][66][70][77][99];

- further efforts focussed on the development of tools and related practical guidance [79] to be used by practitioners in the context of attacker-centric threat modelling;
- development of reusable artefacts and enablement of reusability between models and methods [98];
- consideration of current trends in software engineering, including the integration into agile practices [62][97]; and lastly,
- innovation and integration of new methods (e.g. machine learning in [85] or integration with the cyber kill chain methodology [99]) and extension of methods into other fields (e.g. conflict modelling in [99]).

Nevertheless, a glimpse of the potential of attacker-centric aspects is evident in the reviewed literature sample, e.g. in the area of communication or collaboration. However, the exact value of using attacker attacker-centric thinking and approaches to practitioners seems relatively undefined, with many limitations and question marks remaining, including potential restrictions around employing the mindset of 'thinking like an attacker' for effective modelling purposes. This aspect is also central to the discussion of attacker-centric threat modelling carried out in the next section, looking at structured approaches to identify and assess potential threats using an attacker focus.

2.2 Modelling on attackers: attacker-centric threat modelling

Expanding on the introduction to this thesis, which has introduced the topic of attacker-centric threat modelling, and with the intent to further focus on a specific perspective of attacker-centric security, this section aims to present an theoretical introduction into attacker-centric threat modelling as a subset to threat modelling. To achieve this, an initial definition of threat modelling is attempted, followed by an overview of commonly used foci and their related methods, including attacker-centric approaches as a focal point of this thesis. This is then followed by a note on the diverging opinions around adopting an attacker mindset or 'thinking like an attacker' as previously hinted at.

At this point, it is worth noting that the subject of threat modelling crosses both the academic and commercial domain, with early efforts in the area provided in professional textbooks (e.g. an early attacker list developed by Barnard in his work on intrusion detection in 1988 in [100]), by corporations such as Microsoft (including the frequently referred STRIDE methodology put forward by Kohnfelder and Karg in 1999 [101], *Writing secure code* by Howard and LeBlanc in 2001 [2], *Threat Modeling* by Swiderski and Snyder in [102] which introduced the concept as a comprehensive structured methodology for securing systems or Shostack's *Experiences Threat Modelling at Microsoft* from 2008 [5]) as well as efforts supported by government agencies (like the academic work of Schneier including his proposal of attack trees [80] in collaboration with National Security Agency authors [103]). Key textbooks like *Threat modelling — Designing for security* by Shostack from the year 2014 [6] (or *Risk-centric threat modelling* by Morana & UcedaVelez, 2015 [77]) have been referred to by practitioners and

academic researchers[8] alike. Currently, while threat modelling as a practical and commercial method seems to be well-researched and frequently considered in academic works, it still remains considerably industry-led, with industry vendors publishing blog posts on "real-world threat modelling" [104] or threat modelling next generation 5G mobile communications [105] and several commercial threat modelling tools available at cost (e.g. ThreatModeler [106]). Within this thesis, materials related to threat modelling have generally been selected for their neutral perspective on the topic — where known third-party interest or involvement is present, this has been noted.

2.2.1 Defining threat modelling

To begin with, the term 'threat model' generally means a specific set of threats to a specific system [67], while 'threat modelling' should be understood as a structured methodology and activity [9]. Drawing on the comparative literature review on threat modelling by Xiong & Lagerström [107] and other works systematically introducing threat modelling methods (e.g. [108][109]), a number of threat modelling definitions can be seen to emerge. Containing the elements of a structured approach, attacker goals and overall threat identification as well as a link to mitigation techniques, the definition by Mead et al. in [14] seems appropriate and grounded in business practice: "a threat modelling method is an approach for creating an abstraction of a software system, aimed at identifying attackers' abilities and goals, and using that abstraction to generate and catalogue possible threats that the system must mitigate".

As specific tool support typically plays a role in threat modelling, this element could be added to this definition — Uzunov & Fernandez in [107] for example reference threat libraries or attack taxonomies in their definition of threat modelling. Lastly, threat modelling elements may also be found under related terms, e.g. Tuma et al. [62] use 'threat analysis', however their definition of the term ("activities which help to identify, analyse and prioritise potential security and privacy threats to a software system [...]") is very similar to standard threat modelling definitions as reviewed in Xiong & Lagerström [107]). Similarly, Paul & Vignon-Davillier use 'risk assessment approaches' in their work concerning attack trees [76], whereas Mauw & Oostdijk [69] see attack trees falling under the label of threat analysis, while Meland et al. [9] view them as a threat modelling method in itself.

2.2.2 Threat modelling foci

Three common strategies or foci for threat modelling have generally been agreed on across literature, with a number of methods and tools aligned to them respectively, but all with unique use cases and limitations. It is worth noting that methods and tools may work across the boundaries of these foci definitions (e.g. the *Hybrid Threat Modelling Method* proposed by Mead et al. [14]) or be seen to complement other methods (e.g. attack trees [4][6] ch.4).

[8] To illustrate this, one could consider the large number of references for Shostack's book [6] in academic literature — here, Google Scholar shows a high number (491) of citations across indexed resources. Related works have also been referred to regularly by academic researchers (e.g. Shostack, 2008 [5]: 125 citations; Morana & UcedaVelez [77]: 59).

Asset-/risk-centric methods

Asset-centric approaches are concerned with the protection of assets with the purpose of understanding and managing business risk — deployment patterns and business objectives of the system will most likely be known, with assets and access control understood [110]. While assets can be defined as "a system or user level resource associated with certain value" [8], Shostack ([6] p.37) views them in three overlapping ways: 'things you want to protect' (like the reputation of a financial services company), 'things attacker want' (like credit card numbers) and 'stepping stones to either of these' (any intermediaries or entry points enabling attacks against valuable assets). Asset-centric approaches may be best suited for relatively clearly defined line-of-business applications with rather specific aims [110], as the enumeration of assets in complex, unknown systems may depend on expert knowledge [13], prove time-consuming and ultimately distract from the overall purpose of identifying and mitigating threats. Crucially, asset-centric approaches on their own may lack sufficient structure to enable effective threat identification ([6] p.39), requiring further methodological additions such as lists of common vulnerabilities, attack surfaces or mitigations [12]. An example for this is the risk-centric PASTA (Process for Attack Simulation and Threat Analysis) method, which relies on an "attacker-centric perspective to produce an asset-centric output in the form of threat enumeration and scoring" as described by Shevchenko in [4] (similarly in Nweke & Wolthusen [111]). As asset-centric approaches may often include an element of risk ranking, they can support prioritisation of threats (based on the value of an asset) — additionally, as compliance requirements centre around the protection of assets (e.g. personally identifiable information under the General Data Protection Regulation (GDPR) [56]), they may be helpful in this context. Frameworks aligned to this focus include methods like DREAD, OCTAVE, TRIKE or ISO 27005/31010 [4][13][111].

Software-/system-centric methods

Software-centric approaches look to proactively decompose the existing system or software being built, with the aim of identifying present vulnerabilities and potential attacks to each of the system's components [8][15]. Creating comprehensive software models is seen to be of considerate value in Shostack ([6] pp.42), helping to understand the potential complexity of large-scale systems or multi-component software (including legacy elements) by taking a developer's view. Software-centric approaches therefore also seem suited for systems with an unknown deployment pattern, as they aim to ensure the security of the underlying code [110]. Additionally, software-centric models can be adapted throughout the modelling process to reflect potential mitigations for existing vulnerabilities and test their impact and effect [12]. With the structured decomposition of the system at the centre of such approaches, Shostack for example has suggested a number of visualisation and diagramming tools in this context (see [6] p.44–56), with data flow diagrams (DFDs) being used across a range of approaches — an example of such a DFD for a digital banking environment is shown in Figure 2.4.

As already mentioned in the introduction of this thesis, STRIDE as a mnemonic for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege is another element and methodology found across many threat modelling approaches and studies (see Xiong & Lagerström [107]). Within STRIDE, system decompositions such as DFDs are evaluated for threats using the five STRIDE threat type definitions (refer to Table

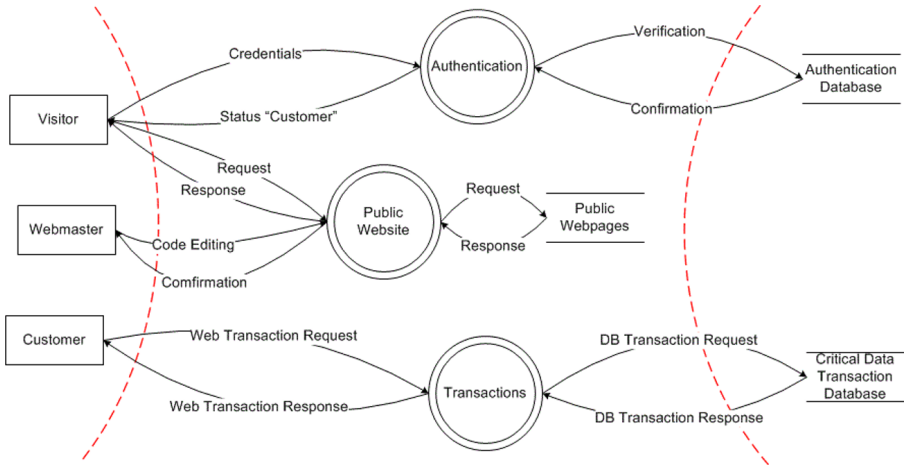


Figure 2.4: ***Data Flow Diagram for a digital banking example [110]***

2.1), with variants of the methodology focussing on threats specific to each element of the system (e.g. data stores; 'STRIDE-per-element') or of each interaction affecting a system (described in tuples of origin/destination/interaction [6] p.80). Indicating its practical value and prevalence, Shostack [6] dedicates an entire chapter (ch.3) to STRIDE, while Bernsmed & Jaatun in [112] also highlight the real-world usage of STRIDE in their study on threat modelling and agile software development 'on the ground' at four Norwegian organisations. In their comparative review of threat modelling methods, Shevchenko et al. [4] at the Software Engineering Institute at Carnegie Mellon even consider STRIDE as the "currently most mature threat modelling method". And using STRIDE as a method for threat identification is compelling — the method is overall accessible (mentioned in [107][4]; while empiric data on this seems sparse, e.g. both Scandariato [109] and Yuan et al. [66] have run small-scale evaluation studies with students for STRIDE and the STRIDE-based Microsoft Threat Modelling Tool respectively with encouraging results in both studies) and tool support is available (e.g. Microsoft Threat Modelling Tool [113]). It can also be adapted and applied to a variety of settings (including cyber-physical systems in Martins et al. [8]).

There are however some drawbacks when employing the STRIDE methodology: especially for complex, large-scale systems with a large number of potential threats, threat enumeration can be time-consuming and challenging for the modeller [14], although tool support or supporting materials may be of use in this context ([6] ch.3). Additionally, Surridge et al. [13] sees software-centric tools as unsuited for analysing trust as human adversarial threats or unintended user actions may not be captured adequately — a combination of methods may help to mitigate this effect. Beyond STRIDE-based methods (also including the Elevation of Privilege card game [6] pp.501), a range of threat modelling methods and tools employing a software-/system-centric focus are currently in existence (e.g. open-source methodologies like LINDDUN or CVSS [4] as well as vsRisk or ThreatModeler commercially [13]). Lastly, threat libraries such as CAPEC, ATT&CK, OWASP Top 10 or SANS Top25 (collected by Hurlbut[9] [21]) may help to learn about specific threats to systems.

[9]Robert Hurlbut as a subject matter expert on threat modelling is associated with the Bank of America at the time of publication, working as a threat modelling architect and lead in the area of cyber security technology [21].

Threat	Violation	Definition	Affected elements
Spoofing	Authentication	Pretending to be something or someone other than yourself	Processes, external entities, people
Tampering	Integrity	Modifying something on disk, on a network, or in memory	Data stores, data flows, processes
Repudiation	Non-repudiation	Claiming that you didn't do something, or were not responsible. Can be honest or false — evidence is key	Process
Information disclosure	Confidentiality	Providing information to someone not authorised to see it	Processes, data stores, data flows
Denial of service	Availability	Absorbing resources needed to provide service	Processes, data stores, data flows
Elevation of privilege	Authorisation	Allowing someone to do something they are not authorised to do	Process

Table 2.1: ***Overview of STRIDE threat categorisation (based on Shostack [6] p.62)***

Attacker-centric methods

Attacker-centric approaches takeh k the adversary's view to identify risks to the system, focussing on their abilities, goals and motivations [110][15], while also evaluating and anticipating potential attack paths attackers may follow to reach their targets [8]. The underlying assumption for these approaches is that such a mindset of 'thinking like an attacker' will provide a "realistic perception of the potential weak points in the system that the attacker is most likely to exploit" [15] — this is seen to help a system designer to decide on appropriate mitigations for the identified vulnerabilities. Attacker-centric approaches may work as a threat modelling focus as a way of 'humanising' risk or communicating with senior stakeholders, making threats seem 'real' ([6] p.40) — Surridge et al. [13] sees them as especially appropriate for identifying threats originating from or involving human elements. In contrast, they are seen as difficult to automate and largely dependent on the knowledge and input of subject matter experts [13], who may introduce their own views and potential bias to the model [7][6] p.40. At the same time, they may also fail to provide enough structure to effectively find threats: modellers may not be able to deduce specific threats based on what is known to them about attackers ([6] p.41) or even miss relevant attackers [114]. Similarly, they may also not decompose the system adequately to show where exactly specific mitigations should be placed to protect potentially affected system components [13].

Despite these limitations, a range of methods and tools with at least a partial attacker focus exist currently. Attack trees, introduced in the last section, as a common way of conveying the attack path an attacker may follow to realise their goal belong to this group [4][80][110]: tools making use of this perspective are e.g. SeaMonster or SecuriCAD [13][95]. The Attack-Defense Tree Tool (ADTool) from Kordy et al. [79] adds the perspective of the defender by enabling the creation of attack-defense trees, allowing the "modelling of large real-life scenarios" [79] together with potential mitigations, "resulting in a holistic overview of a security game" [12]. Attacker-centric methods also include attacker lists and categorisations such as taxonomies and typologies (as described further in Section 2.3): Martin-Vegue for example

has provided a full threat modelling exercise based on the attacker types in the Intel Threat Agent Risk Assessment list in [115]. Attacker personas are another method with a clear attacker focus, e.g. in Atzeni et al. [7] and Faily & Fléchais [27], with Cleland-Huang [116] describing their "personae non gratae" as archetypical malicious users and Denning et al. [117] suggesting their adversary-centred 'security cards' as a gamified approach to encourage brainstorming around security (also in [14]) — this is further described in Section 2.4. Newer approaches in this field build on user stories as a vehicle borrowed from agile software development, defining the intent of (malicious) users to a system as an accessible vehicle to a large number of stakeholders: "as a [Threat Actor] I wish to [Activity] against [High Value Asset] By [Technique]" [118]. Another attacker-centric method that has attracted interest in this context (e.g. in [6][115]), is the cyber kill chain[10] — further practical demonstration and research examples around this are however required at this point in time.

2.2.3 The case for and against 'thinking like an attacker'

Attacker-centric threat modelling may feel like an intuitive, effective approach to many aspiring modellers — yet, Shostack as one of the central figures in the area of threat modelling opposes this approach strongly ([6] pp.40 [5][55]). This section aims to define both sides of the discussion, before ultimately concluding on a nuanced picture in this context.

Interestingly, several examples of research efforts that have assumed an almost inherent benefit to gathering attacker information as part of their motivation, including attacker categorisations like the ones described in this work (in Section 2.3: e.g. Rogers [23] or subsequently Hald & Pedersen [24]). Similarly, Brynielson et al. "assume that a fair view of the threat that attackers pose can help improve cyber defense" as a prerequisite to their work in [120] on attacker personas and their application in cyber defence exercises, without providing procedural detail on how this benefit can be capitalised on.

Others have been more explicit on the value of taking an attacker perspective, still overall treating attacker-centric thinking favourably. Atzeni et al. [7] explain the need for attacker information as follows in this context: as abstractions held about a system may significantly vary between attackers and defenders due to their own past experiences, knowledge and skills, gathering and analysing attacker information may help to understand how the attacker side views the system including potential entry points and weaknesses. In his influential work on attack trees, Schneier [80] supports this view, asking attack trees to be combined with information about attackers, as "different attackers have different levels of skill, access, risk aversion, money, and so on [...]". Cleland-Huang builds her 'personae non gratae' as a tool to support high-level strategic reasoning about potential threats, with the expectation that a "persona non grata with more specific attack strategies to expose vulnerability points of the product" can ultimately be built to support more granular threat modelling activities [116]. Backed up by their work on evaluating the effectiveness of threat modelling methods, Shull

[10]The cyber kill chain, developed and maintained by Lookheed Martin, is a framework of seven distinct stages an attacker is expected to move through to realise an attack (reconnaissance, weaponisation, delivery, exploitation, installation, command & control, actions on objectives) [119]. Shostack has included the concept of kill chains in ch.18 of this book [6] as an 'experimental approach' with future potential.

& Mead [58] take a more explicit stance on the positive value of attacker-centric thinking[11], finding that "threat models built using personae non gratae exhibited a higher degree of consistency than other techniques" (e.g. STRIDE) — they however caution this by ultimately proposing a hybrid threat modelling method (including STRIDE), as "no individual threat model included all identified threats" [58].

In addition to this threat modelling context, the notion of 'thinking like an attacker' is also discussed frequently in the context of academic curriculum design for the subject of cybersecurity and already forms part of many university-level courses (e.g. in [19][20][121][122]. While some level of "consensus that adversarial thinking should be taught in higher education settings" [123] seems to present, this educational paradigm continues to be challenged, with Schneider [124] wondering whether "adversarial thinking for cybersecurity (can) even be taught, or is it an innate skill that only some can develop?" (similarly posed by Schneier, in [125]). Padmos [68] also casts doubt on a unified attacker mindset, questioning whether "a single attitude that allows individuals to think like an attacker" even exists, suggesting a multi-factor mindset to counter this effect (integrating views from various archetypical roles, e.g. analyst, engineer, architect, [...]). At the same time, a "facility in adversarial thinking" is considered an essential thinking ability in becoming a security expert by Dark [125], while "technological capabilities, unconventional perspectives, and the strategic reasoning of hackers" make up the definition of adversarial thinking in Biddle et al. [126], highlighting the challenges of translating these aspects into curriculum design. Outside of an academic context, the attacker mindset of 'thinking like an attacker' has also seen significant uptake and support from the practitioner community in a commercial context, with a number of security vendors advocating attacker-centric strategies publicly, e.g. through corporate blogs [127][128] or other industry-specific media outlets [18][129].

In stark contrast to this, attacker-centric threat modelling has been discouraged actively by a number of authors. In this context, Shostack has been the harshest critic of these approaches over the last decade. As early as 2008, he pointed out that 'thinking like an attacker' does not work for most people, because they simply have "no clue how to do it" [5]. Specifically, attacker-centric approaches and tools like attacker lists or personas may not offer enough structure for all modellers to reliably identify threats according to Shostack, making them inferior to system-centric approaches (as included in his textbook in 2014 [6] p.41). This concern is shared by others, with Surridge et al. [13] remarking that effective threat modelling based on potential attackers to a system will require substantial expert knowledge, demanding a very good, but often unrealistic understanding of potential attackers (also in [13][66][75]). In direct relation, results of such attacker-based modelling efforts are seen as unlikely to be consistent and reproducible [6][77]: for example, experts and stakeholders involved in their creation may disagree over the threats (and attackers) to consider and how to mitigate them [13][114] — additionally, the human modellers may introduce their own

[11]Specifically, the authors evaluated three specific threat modelling approaches in [58] for their effectiveness in threat identification: security cards, STRIDE and persona non grata. Security cards are "an approach that emphasises creativity and brainstorming over more structured approaches such as checklists", while STRIDE aims for "modelling a system and subsystem and related data flows". Like attacker personas in Atzeni et al. [7] or Faily & Fléchais [27], persona non grata representations include "archetypal users who behave in unwanted, possibly nefarious ways" [14].

biased views in relation to attackers to the model [65]. These problems are substantiated by the difficulties around teaching adversarial thinking identified earlier in this section: the immense challenge of learning how to 'think like an attacker' successfully also makes learning how to threat model around this paradigm a difficult task.

Given the apparent disparity in the perception of attacker-centric threat modelling or 'thinking like an attacker', how can the current state for this topic be summarised into a more nuanced picture? Without further enquiries into how such attacker-centric thinking and related approaches are employed in organisational practice, it may be useful at this point to conceptually separate the two aspects of attacker-centric threat modelling and 'thinking like an attacker' as a mindset and supporting tool. While 'think like an attacker' may not prove to be as easily accessible and effective for structured threat modelling as suggested by some, it may still provide substantial value in practice: for example in the area of communications, e.g. to "make the threats real" when working with senior stakeholders [6]. Building on this, Atzeni et al. [7] view data-driven, grounded models of attackers as crucial to counteract existing stereotypes about attackers that system developers and designers may hold — this could be extended to a wider range of stakeholders. Certainly another aspect not to be discounted is the very tangible and engaging nature of working with attackers. Kelsey (in [6] p.403) views 'think like an attacker' as a good starting point "to get people in the mood for threat modelling", while Miller has run the interactive online workshop *Drinks and Persona Building: Creating Adversary Trading Cards* at the 2020 instalment of the OWASP Open Security Summit [130]. In an educational setting, Chothia & De Ruiter [131] confirm this aspect, highlighting how "students [...] liked 'thinking like an attacker' " in their evaluation study on a penetration testing exercise in higher education. To help confirm or revise this overall understanding of attacker-centric thinking and approaches, at least in an organisation context, an enquiry into the value and feasibility of taking an attacker mindset for (financial services) practitioners in their everyday roles is included in Research Objective 6 and Question 5, methodologically prepared for in Section 3.5.4 and documented in Chapter 8.

2.3 (De-)constructing attacker categorisations: taxonomies and typologies

Attacker analysis and profiling have long been part of the analytical toolkit of investigators and date back centuries [132], both for planning defence strategies and to aid forensics post-attack. Researchers have been interested in finding out more about the individuals behind cybercrime since the first illegal activities were observed in the early beginnings of the cyber era, initially in the area of telecommunications. In this context, attacker typologies and taxonomies are commonly used vehicles to represent attacker types and categories applicable to either a specific system or for generic usage.

Early research in the area (e.g. by Gordon [133], Hollinger [134] or Landreth [135]), mostly based on a relatively small number of interviews, documented case studies and anecdotes, indicated variations amongst attackers, for example their technical skills, motives or level of damage done to the system targeted. Such observations ultimately led to the creation

of attacker categories, e.g. the three types of computer criminals (crackers, criminals, and vandals) identified by the FBI in 1997 [59] or Pfleeger & Pfleeger's early taxonomy consisting of amateurs, crackers, and career criminals[12], also from 1997 in [137]. More recent works include the widely referenced work by Rogers [23] from 2006, with nine attacker types and a two-dimensional matrix visualisation aligning attacker motivations and resources. Based on a literature analysis of previous works on attacker taxonomies, individual attacker categories and subcategories, Meyers et al. [42] in 2009 then consolidated research efforts to date into eight common categories of attackers. In 2012, Hald & Pedersen [24] carefully updated known attacker categories, using current terminology and threat properties. More recently, in 2015, Seebruck [25] proposed an updated attacker typology. While closely built on the mentioned earlier works, it has been adapted with the intent to capture "recent increases in ideologically and socially motivated hacking". A comprehensive and critical assessment of the state of attacker typologies and taxonomies can also be found in the 2018 work by De Bruijne et al. [26]. Underlining the applied and varied nature of the research area, research efforts in the area include academic publications (e.g. Hald & Pedersen [24], Seebruck [25], Chandler [138] or Chiesa et al. [93]), government or institutional research (e.g. Meyers et al.[42] or Ivoce [59]), industry-led proposals (e.g. Intel Threat Agent Library [22]) including practitioner literature (e.g. Landreth [135] or Kilger et al. [139]) as well as collaborations across these domains (e.g. De Bruijne et al. [26] or Ziegler & Fötinger [140]).

However, while they certainly provide interesting and accessible visualisations of human threat actor landscapes, attacker typologies and taxonomies suffer from a range of limitations and shortcomings at this point in time, with De Bruijne et al. [26] concluding on "a disheartening picture of state-of-the-art thinking on threat actor typologies" after their initial literature review. For them, problems are mostly methodological, with used data sources, classification and construction methods including evaluation and validation efforts not adequately accounted for. It is felt that many taxonomies seem to be built on each other, reference previous literature rather than using independent real-life datasets [24][42], with key references in the area not meeting certain standards (Rogers [46]: no clear publication date and route, named data sources, methodology or Ziegler & Fötinger [140]: positionality of commissioning company and arising third party interest not clarified). As a further methodological consideration, the introduction [23] and continuous use [24][25] of circumplex models as a highly theorised concept from clinical psychology and sociology shows limited theoretical grounding.

2.3.1 Common terminology: taxonomy vs. typology

Attacker categorisations in literature use a number of specific terms for their various elements, starting with differing labels for the classified subjects. Many older categorisations [134][135] and the ones building closely on Rogers [46] use the term 'hacker' ([24][25]; or 'cracker' in [59],

[12]Pfleeger & Pfleeger maintain this categorisation of computer criminals in the second and third edition of their textbook *Security in Computing*, while their later editions have been updated to hackers, terrorists, criminal-for-hires as well as individuals, organised crime members and loosely connected groups [136] accordingly.

Pfleeger [137] initially uses 'criminal'), while newer propositions use more abstract terms such as 'cyber adversaries' [42], 'threat agents' [22], 'attackers' [136] or 'actors' [26]. Similarly, the usage of the more neutral, all-encompassing term 'attacker' is suggested for this thesis.

While many categorisation efforts do not use an explicit label (e.g. Pfleeger et al. [136] simply refer to attacker 'types'), there seems to be a split between the usage of the terms 'typology' and 'taxonomy' to describe classification frameworks, with little reflection on why one was chosen over the other. While categorisations referring to Rogers [46] or the Intel Threat Agent Library [22] have maintained the usage of 'taxonomy' (e.g. [24][42]), latest efforts have reflected more critically on this and suggested the use of 'typology' as more fitting. The two terms can be clearly distinguished, with Da Silva [141] stating that "conceptually developed configurations are defined as typologies, while empirically derived configurations are defined as taxonomies" (also found in Bailey [142], a commonly cited primer on taxonomies and typologies from a social sciences perspective). Seebruck [25] support this by viewing taxonomies as categorising "dimensions based on empirical observation and measurable traits". In direct contrast, typologies can be viewed as a non-exhaustive, "conceptually derived interrelated sets of ideal types" [26] p.9. For the purpose of the introduced categorisation of digital banking attackers in this thesis, the adoption of the term 'typology' is suggested. This follows the reasoning that this categorisation is likely to be non-exhaustive and present ideal summaries of attacker groups rather than present truly empirical, in-depth and formally measurable attacker characteristics from a complete, finite dataset.

2.3.2 Value and purpose of attacker categorisations

When it comes to the underlying reasoning behind the creation and maintenance of attacker categorisations, key works in the area of attacker categorisations are largely in agreement over their purpose and value. At a strictly formal level, De Bruijne et al. [26] view the format of a typology as "appealing because it promises to yield a concise yet parsimonious framework to describe and classify observed patterns". Simply put, attacker categorisations such as typologies and taxonomies are seen to help identify, structure and classify information gathered on attackers [25], establishing a common reference point and standard vocabulary where possible [22]. Hence, at the most basic level, authors generally agree on categorisations supporting a better understanding of adversaries and helping with the aim of "imagining the full landscape of possible attacks" [136] and "knowing your enemy" [23][24][25][46][143]. Early categorisation efforts (e.g. [46][137]) have also highlighted the initial realisation of the heterogeneous nature and diversity of existing attackers (as opposed to there being a "typical" computer criminal [137]) as a further benefit gained from attacker categorisations, with Gordon [133] supporting this in her study on virus writers as a unique attacker group.

But how can this theoretical understanding obtained through such categorisation efforts then be translated into tangible benefits applicable to security practice? Here, Hald & Pedersen [24], Seebruck [25] and the Intel Threat Agent Library [22] mention the definition of common, up-to-date terminology in this area as crucial for shareability and collaboration initiatives, together with avoidance of duplication of efforts and gains in efficiency by using attacker lists or threat agent libraries (in [22]). De Bruijne et al. [26] define the goals for their

typology as an update to previous typologies forming part of a large-scale security assessment exercise (*Cyber Security Assessment Netherlands* in their case), used and contributed to by security analysts in both public and private organisations. However, most reviewed materials remain relatively open-ended in regard to the exact purpose of the provided taxonomies, e.g. in [59] "for the sake of classification and tracking" or very specifically stated in [22]: "our agents do not represent specific individuals, and our library is not intended to identify individuals or to be used for investigating actual security events". Similarly, Shostack [6] sees attacker categorisations as an unspecific, but useful resource for security professionals, including example attacker lists and personas in his key textbook on threat modelling to supplement other structured, asset- or system-centric approaches. In contrast, Ziegler & Fötinger [140] regard their enquiry into the psychology of attackers mostly as an attempt to close a gap in literature.

Overall, much work in this area seems to be theoretically and methodologically driven, with taxonomies and typologies directly extending and building on each other (e.g. [24][25]). With the distinct exception of De Bruijne et al. [26], attacker categorisation works seem to be high-level, generic representation aiming to theoretically highlight the variation of attackers, their motives and potential modus operandi rather than very specific, ready-made models to be used in practice by security analysts (although they may inform and support these practical perspectives). However, this is not to deduct their overall value — they provide both common language and fundamental knowledge around attackers and may serve as reference points for further development of customised risk assessments and threat modelling.

2.3.3 Categorisation criteria in prior taxonomies and typologies

Efforts to label and categorise attackers in cybercrime aim to take a distinct perspective to identify variations within the entire population. For this, one or multiple criteria are employed as a lens to distinguish attacker characteristics and to help build clusters of similar attackers — an overview of criteria extracted from previous literature is shown in Table 2.2.

Across works ranging over the last two decades, motivation and resources (including skills, funds and others) can be seen as the major two criteria for categorising attackers (as evident in Table 2.2). Pfleeger [137] in his early taxonomy from 1997 describes three attacker types (amateurs, crackers and career criminals) entirely around these two criteria, with Rogers in 2006 also building his two-dimensional classification model on these two criteria [23]. Other researchers such as Landreth [135], Ziegler & Fötinger [140], Kilger et al. [139], Meyers et al. [42], Hald & Pedersen [24], Long & Hadsell [143] as well as recently Seebruck [25] support this view. However, different to this, Ivoce [59] in 1997 use motivation as the main distinguishing factor between his attacker types (cracker, vandal, criminal). Motivation and intent as attacker descriptors feature in most categorisations: these motivations may be of financial nature or based on revenge, curiosity or notoriety (e.g. [59] or [135]), but motivation can also be found in cause and ideology (e.g. [144] or [136]). Skills and resources may refer to factors such as time and funds available to the attacker, technical skill and capabilities of the attackers, but also fewer tangible features such as initial access options, insider knowledge and personal connections available to the attacker (in Parker et al. [144]).

Criteria	Reference in literature
Motivation, intent	Landreth, 1989 [135]; Ivoce, 1997 [59]; Pfleeger, 1997 [137]; Rogers, 1999 [46]; Kilger et al., 2004 [139]; Parker et al., 2004 [144]; Ziegler & Fötinger, 2004 [140]; Rogers, 2006 [23]; Intel Threat Agent Library [22]; Meyers et al., 2009 [42]; Hald & Pedersen, 2012 [24]; Long & Hadsell, 2012 [143]; Seebruck, 2015 [25]; Pfleeger et al., 2015 [136].
Resources (skills, funds and others)	Landreth, 1989 [135]; Pfleeger, 1997 [137]; Rogers, 1999 [46]; Kilger et al., 2004 [139]; Parker et al., 2004 [144]; Ziegler & Fötinger, 2004 [140]; Rogers, 2006 [23]; Meyers et al., 2009 [42]; Hald & Pedersen, 2012 [24]; Long & Hadsell, 2012 [143]; Seebruck, 2015 [25]; Pfleeger et al., 2015 [136].
Level of danger posed	Hollinger, 1988 [134]; Rogers, 2006 [23]; Chiesa, 2008 [93]; Meyers et al., 2009 [42]; Chabrow, 2012 [145]; Long & Hadsell, 2012 [143].
Modus operandi	Ziegler & Fötinger, 2004 [140]; Chiesa, 2008 [93]; Meyers et al., 2009[42]; Hald & Pedersen, 2012 [24].
Activities	Hollinger, 1988 [134]; Gordon, 1996 [133]; Rogers, 2006 [23]; Intel Threat Agent Library [22].
Other factors (e.g. own traceability)	Gordon, 1996 [133]; Kilger et al., 2004 [139]; Ziegler & Fötinger, 2004 [140]; Rogers, 2006 [23]; Intel Threat Agent Library [22]; Hald & Pedersen, 2012 [24]; Xu et al., 2013 [146]; Pfleeger et al., 2015 [136].

Table 2.2: ***Criteria for categorising attackers in existing literature***

There are other frequently used criteria for classifications, often supporting the main criteria of motivation and resource (refer to Table 2.2). The level of danger posed by an attacker, which may be described as the amount of damage caused to a specific system, group of users or individual users, can also be employed to categorise attackers. This categorisation criterion is indicated by Chiesa et al. [93] in their review of attacker categories, but also used in Chabrow [145] and in the early taxonomy by Hollinger [134], where a difference between attackers only exploring systems or actively stealing information is made. The methods employed to attack a system ('modus operandi') can also be used as classification criterion. Hald & Pedersen [24] employ a set of threat properties in their taxonomy which includes this dimension, a view supported by Chiesa et al. [93] and Chabrow [145]. Directly related, activities in which an attacker is involved may also categorise them — Hollinger [134] mentions groups specifically committing copyright infringements, while the work by Gordon [133] focuses on virus writers.

Less used criteria include for example moral value and judgement — Xu et al. [146] use them as distinguishing factors between criminals, grey or white hat hackers. In Ziegler & Fötinger [140], attackers were asked whether and to what extent they were aware of their own traceability (similar to visibility used as a criterium in the Intel Threat Agent Library [22]), providing another factor for differentiating attackers (also in Parker et al. [144], who refer to the attacker's attitude to risk). Group structures and affiliations may also be part of an attacker categorisation: e.g. in Pfleeger et al. in their later attacker classification in [136], where individuals and organised worldwide crime groups are distinguished (also in [139][144]). For her specific review of virus writers, Gordon [133] relies on criteria such

as ethical development and maturity, resulting in categories ranging from 'adolescents' over 'college students' and 'adults' to 'ex-writers'. The extensive threat agents library in [22] also divides threat agents into either 'non-hostile' or 'hostile' — for attacker categorisations like in this work, attacker types can generally be assumed to be hostile, in contrast to e.g. untrained employees causing damage by human error as a threat agent.

In summary, and as indicated in Table 2.2, motivation of the attacker paired with their resources can provide an effective description of an attacker type. Other criteria such as the level of danger posed by the attacker, the employed modus operandi and activities involved can provide further detail to the attacker profile. This approach is, for example, taken by Meyers et al. [42], who list skill level, maliciousness, motivation and method for each attacker type in their proposed categorisation.

2.3.4 Common attacker types found in previous literature

This section presents a consolidated view of prior attacker categorisations and their included attacker types — this exercise has also been undertaken in Meyers et al. in 2009 [42] and is updated and extended here. A consolidation seems warranted as attacker categorisations differ not only in the underlying criteria (as outlined in the last section) and the sources they are based on (such as the researcher's experience or interviews with real attackers). They also vary in their terminology (such as labels used for attacker types) and the overall number of attacker types. However, while keeping these variations across categorisations in mind, it is possible to identify clusters of similar attacker types. These eight groups of common attacker types are presented in the remainder of this section, including their main characteristics such as motivation, resources and level of danger posed as well as the various terms used for their description by different researchers. From prior literature sources as mentioned in Table 2.2, a consolidated overview of common attacker types as described in literature is produced in Table 2.3 at the end of this section.

Novices group

Attackers with limited technical skills and other resources can be found in most categorisations, labelled 'novices' (e.g. in Landreth [135], Rogers, 2006 [23] and Seebruck [25]), 'amateurs' (Pfleeger, 1997 [137]), 'newbies' (Rogers, 1999 [46]), 'losers and lamers' (in Chandler [138]) or 'script kiddies' (in Chiesa [93], Chabrow [145] and Hald & Pedersen [24]). Their motivations are largely curiosity and thrill seeking, but also gaining a reputation amongst their peers (especially for 'script kiddies') — financial gains from breaking into well-protected systems cannot be expected due to their limited hacking skills, keeping the overall danger levels posed relatively low. While they may decide to employ prefabricated tool kits to execute certain attacks, limited funds will not enable them to purchase highly dangerous, more expensive kits. This group is however by no means homogeneous — some 'script kiddies' for example will show more advanced skills and hence pose more danger. Overall, this group includes attackers with limited funds and experience — they may or may not transition into more advanced categories at a later stage.

Browsers & cyber punks group

Attackers with low to moderate skill levels, funds and resources make up this group — their motivations however may slightly differ. Both Hollinger [134] and Landreth [135] introduced early on the concept of 'browsers' and 'students', who will illegally access a system to study it in detail and view breaking into the system as an intellectual challenge and something to 'brag about'. Their aim is to remain undetected and these usually benign attackers normally pose little danger. A variant of these categories is the 'tourist' also defined by Landreth [135] — while mostly benign, this attacker type shows little respect for the owners or creators of the system. Although they will most likely not abuse their knowledge about the system in a malign way, they may distribute information on how to access a system to criminals. 'Cyber-punks', 'punks' or 'pranksters' (in Rogers, 1999 [46], Meyers et al. [42] and Seebruck [25]) are another label in this category, describing attackers motivated by thrill seeking and possibly revenge, but also personal gain. They often use prefabricated crimeware kits and may engage in minor fraud activities to fund themselves, but usually have no intention to cause long-term harm. With its combination of attackers with varying degrees of criminal intent, this cluster can be said to be defined by low to moderate skill levels and resource.

Ethical hackers group

This group is one of the most precisely defined clusters, which is relatively consistent across several taxonomies (Chiesa [93], Rogers, 1999 and 2006 [46][23], Long & Hadsell [143], Hald & Pedersen [24], Meyers et al. [42] and Seebruck[13] [25]), represented by labels such as ethical hacker[14], 'white hat' or 'grey hat' and 'old guard hacker' — individuals driven by passion, wanting to gain respect and the search for an intellectual challenge, highly skilled but with no regular criminal intent. While the level of danger posed by such attackers is limited due to their non-malicious intent, they may choose to publicise vulnerabilities endangering not only the security of a system, but also causing potential reputational damage. However, as Chiesa [93] remarks, these attackers may cooperate with the system owner to help mitigate found vulnerabilities (e.g. through bug bounty or responsible disclosure programmes). This group is therefore generally defined through their intact moral code, ethics and ideology and their high skill levels.

Insiders group

Attackers with insider knowledge or access to a system, referred to as 'internals' or 'insiders' form this group, which is consistent across many reviewed taxonomies (such as Rogers, 1999 and 2006 [46][23], Meyers et al. [42], Hald & Pedersen [24] and Seebruck [25]). 'Industrial spies' (as defined in Chiesa [93]) may also fall into this category and be paid to disclose their insider knowledge to third parties. Insider attacks are discussed widely in information security

[13] Seebruck uses the term 'coder' in his taxonomy to describe "non-malicious hackers with upper-intermediate skills who seek prestige" and "non-malicious coders, e.g. white hat hackers". As the term 'coder' has a different meaning in earlier taxonomies (e.g. in Rogers, 1999 and 2006 [46][23]) to describe malicious intruders and code writers, it is not introduced in the ethical hacker category to avoid confusion.

[14] It is worth noting here that 'ethical hackers' can be viewed as both 'white hats' (usually security experts tasked and authorised by organisations to test their systems) or 'grey hats' (who independently seek to challenge a system without a malicious intent). Meyers et al. [42] and Seebruck [25] mention 'white hats' in their taxonomy papers, while others use 'grey hats' or 'old guards' [23][24]. Both approaches are valid — the author takes the view that for attacker taxonomies, the modelling of independent, unaccounted attackers is most interesting and would therefore see ethical hackers as grey hats in this particular context.

as they are seen to account for a large percentage of attacks against organisations (Power, 1998, in Rogers, 1999 [46]). Insiders, often disgruntled or former employees, are motivated by revenge or financial gain and will engage in sabotage, theft of intellectual property and fraud against their (ex-)employer (in Hald & Pedersen [24]; with Ivoce also including this type of potential inside attacker under the label of 'vandals' in the 1997 FBI taxonomy [59]). This is enabled by their specific knowledge about the organisation and the processes within — they may also possess elevated access rights. Their motives, significant amount of criminal intent and these special resources result in a relatively high level of danger posed.

Hacktivists group

The term 'hacktivists' (in Hald & Pedersen [24], Chabrow [145] and Seebruck [25]) is based on the original terms 'cyberterrorists' and 'political activists' proposed by Rogers in [46][23] and also confirmed by Meyers et al. [42]. In the early FBI taxonomy, the 'vandals' attacker type may also fall under this category, with "motivations of electronic vandalism often [...] rooted in revenge for some real or imagined wrong" (Ivoce [59]; also spanning across into the 'insiders' category as mentioned above). Generally, 'hacktivists' refers to groups of attackers engaging in attacks with a political or social background, motivated by ideology, cause and potentially the search for fame. Their campaigns have attracted a lot of publicity in recent years, for example the large-scale DDoS attack by the hacker group 'Anonymous' [147] against legitimate corporations such as Visa, MasterCard or PayPal ('operation payback'). While their intentions may not be aimed at gaining personal financial advantage, their actions may cause huge levels of disruption and destruction of the attacked systems, resulting in enormous financial losses to companies and governments — a criminal element and general disrespect of authorities can certainly be found in this attacker type. These attacker groups can usually rely on a large global network to support them through funding and other resources, and a range of hacking skills can be expected to be found across the group.

Crackers & coders group

This cluster consists of a number of different attacker types, including attacker types with labels such as 'crackers' (Pfleeger [137], Hollinger [134], Ivoce [59] and Chiesa [93]), 'crashers' (Landreth [135]), 'sport intruders' (Power, 1998, in [46]) and 'malicious hackers' (Parker, 1998, in [46]), but also 'virus writers' and 'coders' (Rogers, 1999 and 2006 [46][23], Gordon [133]) as well as 'elite hackers' and 'black hats' (Chandler [138], Adamski, 1999 in [23] and Long & Hadsell [143]). While these attacker types may vary regarding their level of technical skills and resources in terms of funding and equipment, they can generally be considered as very capable and knowledgeable individuals with a high potential for destruction. This group is also united by common motives behind their attacks: they will hack to feed their ego and for entertainment, but also to gain a certain reputation and status within their peer group. This poses a strong contrast to the next group, the professional criminals, where the main motivator is of a financial nature. There are some overlaps between these categories, as elite or black hat hackers may also engage in financial fraud, but generally this group is characterised by relatively high skill levels and a great danger potential with no primary focus on personal financial gain.

Professional criminals group

Professional criminals can be found across many categorisations — as 'thieves' (Landreth [135]), 'career criminals' (Parker, 1998, in [46]), 'darksiders' (Adamski, 1999 in [23]), 'professional criminals' (Ivoce, 1997 [59], Rogers, 1999 and 2006 [46][23], Meyers et al. [42], Hald & Pedersen [24]; 'career criminals' in [137]) and 'organised crime groups' (Chabrow [145] and Pfleeger et al. [136]). Attackers in this group are entirely financially motivated and show high levels of criminal intent. Attackers in this group are likely to be part of larger structures in the form of organised criminal gangs, giving them access to significant resources such as funding and technical skills — also through employing highly skilled individuals to write customised malware for their attacks. This group is defined by its criminal background and professionalism, motivated by the prospect of large financial gains — there is a distinct difference between attackers driven by ego, curiosity or ideology and the criminals engaged in cybercrime found in this category. Other labels in this area include 'hired guns' (Rogers, 2006 [23]), 'information or cyber warriors' (Chiesa [93], Rogers, 2006 [23], Hald & Pedersen [24], Seebruck [25]), which will engage in industrial espionage, website defacement and other illegal activities for monetary compensation. Hald & Pedersen [24] (also in [23]) mention 'petty thieves' — medium-skilled, financially motivated attackers which may have moved into cybercrime from traditional crimes, following targets from offline into online settings.

Government agents group

Also described by the term 'nation states' (Chabrow [145], Hald & Pedersen [24]) or 'foreign intelligence' (Power, 1998, in [46]), state-sponsored hackers form the 'government agents' cluster. These highly skilled attackers are employed by government agencies for the espionage, counterespionage and information monitoring of governments, individuals, terrorist groups and critical infrastructure providers (gas, electricity or water) as well as the financial or defence sectors (Chiesa [93], p.56). Attackers in this cluster will have access to a vast amount of knowledge and funding due to their backing from government or government related institutions. Their appearance, general nature, targets and modus operandi may vary greatly. While examples have been made public in the past, this attacker type largely operates in the underground and not much is known about the actors themselves — examples include the case of the German government trojan ('Staatstrojaner', Chaos Computer Club [148]) or espionage between governments (e.g. China and Australia [149], Russia and UK/US [150]).

Group	Labels	Motives	Criminal Intent	Resources	Activities	Level of Danger
novices	novices, newbies, losers, lamers, script kiddies, amateurs	notoriety, curiosity, thrill seeking and reputation	none to low	limited skills and funds	usage of toolkits	low, but varies across the group
browsers and cyber-punks	browsers, students, tourists, cyber-punks and pranksters	intellectual challenge, but also financial gain	low to moderate, no long-term harm intended	low to moderate skills and funds	adaptation of prefabricated tools	medium, losses through credit card fraud possible
ethical hackers	grey hats, old guard and ethical hackers, (white hats)	intellectual challenge, passion	low, potentially disrespect for rules and authority	high skill levels, funds vary	aim for undetected access to a system	low, may even support owners in improving their system
insiders	insiders, internals, disgruntled employees, (vandals)	revenge, financial gain	moderate to high	moderate skill levels, funds vary, specialist resources	usage of insider knowledge	high, industrial espionage also possible
hacktivists	hacktivists, political activists, anarchists, terrorists, (vandals)	cause, ideology, revenge, but also status, ego	moderate to high	moderate to high skill levels and funding	social, political background to attacks	high, significant levels of damage and destruction
crackers	crackers, crashers, sport intruders, malicious hackers, (virus) writers, coders, elite and black hats	status, ego, entertainment	moderate to high	high skill levels, funds will vary	illegal access to a system, limited fraud, write scripts, mentoring	high, significant levels of damage and destruction
professional criminals	thieves, career criminals, darksiders, professional criminals, organised crime groups, petty thieves, cyber and information warriors	financial gain	high	high skill levels and funding	professional cybercrime activities and financial fraud	high, significant levels of damage (financial losses)
government agents	nation states, foreign intelligence, government agents, (cyber warriors)	ideology, cause	high	high skill levels and funding	espionage, counterespionage and information monitoring	high potential, limited evidence and confirmed cases to date

Table 2.3: ***Consolidated view of common attacker types (sources in Table 2.2)***

2.4 Representing the human attacker: attacker personas

This background section introduces the concept of personas, including a detailed definition from literature as well as a brief indication of potential shortfalls of the method. This level of detail is seen as beneficial to help grasp a basic understanding of the persona method before applying it to attackers in a security context, but also to underline the relative maturity of the method in a design and human-computer interaction context. This is then followed by a brief note on past research involving attacker personas.

The term 'persona' derives from Latin, signifying a concealing mask in contrast to a face for the Romans — this distinction was not present in early Greek philosophy, where πρόσωπον ('prosopon') comprises both meanings [151]. For their work on personas in game design, Canossa & Drachen have written a multi-faceted introduction into the origin and history of personas in [152], positioning personas as "social masks" and roles humans will play in a social context ('the stage of life'; from Goffman in [152]), but also referring back to Weber's *Idealtyp* from social sciences. As a "pure mental construct used to assess the behaviour of social group", ideal types as a theoretical analytical device are concerned with the "stylisation or accentuation of essential features in fact, allow for the synthesis of research acquisitions in order to extract the fundamental characteristics or to elaborate an abstract model with which the ducts can be compared" [153] — they are seen as suitable to be used for terminological, heuristic and classificatory purposes [154] in sociologist analysis and research. Weber himself has put forward early versions of classic personas in their cultural settings, showing the *Lebensführung* as a practical and ethical 'conduct of life' for personalities such as e.g. the puritan associated with a protestant sect or the bureaucrat in an administrative office (as described by Hennis, 1988 in [155][156]).

User persona modelling was introduced and explained comprehensively by Cooper in the influential work *The inmates are running the asylum* in 1999 [157], which argues that technology is all too often not designed with real users and their usage patterns in mind. Personas[15] are realistic, but made-up representations of users from the user community. While user personas are not real users, they represent these throughout the design process. And although they are made up, they are defined with rigour and precision as "hypothetical archetypes of actual users" [157] p.124.

Similar definitions can be found in later research: Norman [158] includes the purpose of user personas in his definition and describes them as an "artificial person, invented for the purpose of helping a designer understand the people who will be using the product". Adlin & Pruitt [28] support this view, calling user personas "fictitious, specific, concrete representations of target users". Dix et al. [159] add to this using "a rich picture of an imaginary person who represents your core user group" as a definition and Bagnall [160] refers to a user persona as "a fictional character made to represent an archetypal user, and is best derived from field

[15] In the field of human-computer interaction and user experience research, the term 'personas' is usually understood to mean 'user personas' (personas representing users of a system). To avoid confusion, the term 'user personas' is used in this work to distinguish them from 'attacker personas'. Where the term 'personas' on its own is used, the general concept and method of personas is meant.

research". Sharp et al. [161] define user personas as a "rich description of typical users of the product under development that the designers can focus on and design the product for". Nielsen in 2013 [30] adds that user personas should be "described in a way so that the reader can recognise the description and believes that the user could exist in reality".

Derived from this selection of definitions, the following factors seem to best define and explain user personas:

- They are of hypothetical and fictitious nature.
- They represent actual target users.
- They are intended to help the designer understand and focus on users.
- They are derived through practical research.
- Their representation is rich, detailed, concrete, specific and near realistic.
- They are presented as characters that readers can relate to and believe to be able to exist in reality.

As with all methodologies, user personas are not without perceived drawbacks, practical problems and theoretical criticism. At the most basic level, the general idea behind personas, the representation of real users through archetypes, is subject to criticism. After all, personas are not real users, leading to questions about their explanatory power and significance in the context of user testing. These problems are closely related to the underlying data being used for the creation of the personas: if no sufficient evidence is employed to back up the personas, credibility and usefulness of the personas decline significantly. Designers and developers then risk relying on stereotypical representations with no relation to real users, as highlighted in Turner & Turner [162]. Other potential problems may lie in the persona representation itself, including too abstract and impersonal representations, but also too many personifying details, which may potentially be misleading [163]. Additionally, the organisational context in which the user personas are employed may hinder the optimal uptake and usage of user personas, for example through not readily accepting, misusing or misunderstanding the concept — Blomquist & Arvola provide an informative account of practical issues faced by a corporate design team when using the persona method [164].

Over the last decade, the notion of an 'attacker persona' (with different labels in existence as included in the following) has been introduced in several academic projects, depicting personas with potentially malicious intent towards systems, their owners and users. One of the earliest efforts in the area is a list of 'threat personas' engaged in defined threat scenarios attacking legitimate systems and users put forward by Aucsmith et al. from 2003 (in [6] p.481) — while described as empirical and grounded in FBI cyberattack data, no exact guidance on attacker persona creation or data sources have been made available to the knowledge of the researcher. In 2008, Steele and Jia proposed 'anti-personas' and 'anti-scenarios' to embody the behaviour of attackers in [44], largely basing their comprehensive work on assumptions about attackers — this distinction between 'assumption personas' (personas capturing assumptions about the target population present in an organisational setting [28] p.40) and their "empirically grounded counterparts" (personas grounded in data) is also acknowledged

by Faily & Fléchais [60] in 2010. Addressing the problem of justification ('rationale capturing problem') underlying these assumptions, they have written comprehensively about *Toulmin's Model of Argumentation* as a structure for logical reasoning about the validity of arguments such as claims from secondary sources to inform persona characteristics in [60] (also in [96] p.123). Also acknowledging the relative difficulty of gathering empirical data directly from the malicious user (attacker), Atzeni et al. in [7] suggest the usage of an approach close to assumption personas and recommend open source intelligence data as a "suitable proxy" in combination with third-part attacker taxonomies (e.g. the Intel Threat Agent Library [22]) to build personas. Tariq et al. [45] in 2012 have aligned their attacker types for organised cybercrime closely to the work of Atzeni et al. [7], using secondary data sources "from a combination of ethnographic studies, psychological studies of attackers, and IT security literature", but have emphasised the element of storytelling and narratives to their personas, also detaching them from a specific context (in contrast to context-bound personas [7][60]).

A number of converging methodological approaches for attacker persona creation have been suggested, in principle borrowing from user-centred design approaches to build traditional user personas — Faily base their used steps "loosely" on Adlin & Pruitt's work ([28]; in [96] p.119), while Dupree et al. rely on the practical guidance on building personas for the web by Mulder & Yaar in [165]. The initial data source selection is followed by a line-by-line data analysis to identify assumptions about attacker types, which are "not elicited verbatim from the text, instead they need to be inferred from the fragments of behaviour that can be reasonably assumed" [7]. In this context, grounded theory analysis as a method has been used in several related works: without further methodological detail, Faily & Fléchais [27] use grounded theory to code a small number of interview transcripts with expert users and stakeholders, inducing "a model of salient grounded concepts and their relationships". Dupree et al. use conventional thematic analysis in their case study on privacy and security concerns to evaluate data from 32 interviews (with mostly student participants) in [165], resulting in the proposal of five personas, representing a range of skills and motivation levels.

The most comprehensive treatment of grounded theory specific to (attacker) personas is however provided by Faily & Fléchais [166] in their work on *Persona Cases: A Technique for Grounding Personas* (also included in [96] p.126), aiming to validate proposed personas and to address the semantical gap between original empirical data and persona representations via a three step approach: summarising propositions and core concepts from the grounded analysis; arguing characteristics by enumerating e.g. backing, modal qualifier and possible rebuttals (also based on Toulmin's work) related to all claims supporting each persona; and lastly, writing supporting persona narratives. If more than one persona is required to represent the characteristics identified, affinity diagramming may help to recognise inherent groupings. Affinity diagramming[16] is an activity found throughout research efforts surrounding attacker personas (e.g. in [7][27][47][165][166][167]), where references to attacker characteristics and behaviours are physically (e.g. using sticky notes on a whiteboard or wall) clustered together, usually in an interactive, collaboratively exercise.

[16] Affinity diagramming is also used to support the categorisation processes within this thesis and are therefore described in further detail in the research procedures in Section 3.5.2 on p.79.

Newer studies in an academic context have continued to build and extend the earlier works and methodological groundworks by Faily & Fléchais [7][27][60][166], for example Ki-Aries (with Faily as co-author) in 2017 [167] proposing a 'persona-centred security awareness solution' and also testing this approach with a case company — while the method is outlined in detail, no complete persona set is provided in this context. Similarly, Altaf et al. in their 2019 assessment of security, safety and human factors issues for railway infrastructures also refer specifically to attacker personas as a supporting tool, but show no further detail on the personas in [47]. At this point in time, detailed documentations of attacker personas seem limited — as a relative exception, Dupree et al. [165] in 2018 have provided a full set of personas in the appendix of their grounded theory based work around users of privacy and security tools.

In a practical context, attacker personas have recently found inclusion in textbooks and conferences primarily aimed at practitioners. Also referring back to Aucsmith's personas as referenced earlier in this section, Bell et al. [168] in their 2017 work on agile application security briefly introduce the idea of attacker personas or 'anti-personas' together with attacker stories as a useful tool to capture security requirements in agile-based team environments. Oldham & Huggins [169] take this further and have presented an interactive workshop on threat persona creation at the 2020 Open Security Summit, also proposing a related scoring system to enable threat prioritisation for developers. At the same event, Miller [130] used personas in the context of a social event (collaboratively creating 'adversary trading cards'), also emphasising the highly engaging, 'fun' nature of personas.

In summary, the body of research around attacker personas is compact, deriving from user-centred design research on personas, but also strongly defined by certain key works and authors (e.g. [7][27]), with only limited full end-to-end examples published. Prior works have emphasised the value of user-centred design methods for building personas in the context of attacker personas, establishing them as a particular variant of persona. Faily & Fléchais [166][96] have also highlighted the importance of grounding (attacker) personas in data, ideally using structured, logical validation and documentation strategies. These findings have been considered in the research procedures in Section 3.5.3 to prepare for the creation of attacker personas in Chapter 7, in response to Research Objective 5 and Question 4.

2.5 The case of digital banking in literature

Forming the last part of this literature review and conceptually moving away from attacker-centric perspectives and approaches, this section focusses on the practical lens applied in this thesis: the case example of digital banking. To introduce the topic, a definition of digital banking as understood within this work is given. As a key theme in literature around the topic, the interaction of usability and security aspects as reflected in previous literature is examined. This is followed by a note on the treatment of dgital banking attackers in previous works. This section also prepares directly for the grounded theory analysis methodologically set out in Section 3.1.2 and undertaken in Chapters 4 and 5, supporting an 'informed grounded theory' to develop a level of theoretical sensitivity rather than adopting a 'delayed literature review' as demanded by early grounded theorists (e.g. Glaser & Holton [170]; Table 3.1).

2.5.1 Defining digital banking

Digital banking as a term seems readily accepted and understood by practitioners and also academics — authors of reports (e.g. from McKinsey [171] or universities like Harvard or St. Gallen [172]) and academic studies (e.g. Mbama et al. [173] interviewing senior UK banking practitioners on the impact of digital banking on customer satisfaction and financial performance or Larsson et al. [174] on the relationship between digital banking and customer loyalty in Sweden) focussing on digital banking haven't seen the need for explicit efforts to define the exact nature of the concept. However, it is felt that for the purpose of this thesis, providing a precise definition will help to prepare the arguments made in the following chapters. Further to that, practitioners Ginovsky [175] and Epstein [176] both agree on a level of vagueness and disambiguity regarding a practical definition for the term — an inconsistency in understanding the term is also evident in the survey amongst banking practitioners by consulting company Celent [177].

Before moving on to the definition, it is worth noting that several banks use the term 'digital banking' to label their online banking services, using the term synonymously with online or internet banking (e.g. Royal Bank of Scotland, UK), although some will include all their online channels (e.g. Nationwide in the UK: mobile, internet browser and smartwatch). In contrast to this, the definition given here focusses on the overall topic rather than naming conventions used by individual companies.

To shape an initial working definition for digital banking, the following elements from current discussions on the topic should be considered:

Basic online banking service provision — firstly and at the most fundamental level, digital banking will still perform standard basic services such as accessing accounts and transactions, for example via mobile channels (banking apps) or online banking (desktop view, in browser). These services are expected to be seamless and fully fulfil (or exceed) customer expectations (in [176], also in PricewaterhouseCoopers [178]).

Focus on customer experience — beyond the provision of basic services, digital banking is also considered to enhance customer experience and make customer–bank relationships more effective and efficient [175][177]. Specifically designed mobile and online applications can help to support this customer focus, by providing innovative, useful and customisable experiences (e.g. in Lipton et al. [179] or Winnefeld & Permantier [180]).

Digitisation of services — digital banking also aims to digitise certain banking services, for example migrating transactions from banking branches into digital channels [177]. Further digitisation is expected to result in lower operating costs, reduced errors and enhanced services [176], for example faster transactions.

Digitalisation of business models — digital banking is also seen to go beyond the relatively simple digitisation of services: it aims to significantly change the business model of banks in line with technological advancement and changing customer needs. Banks may display different business models or stages with regard to digital banking, from basic digital channels, digital subsidiaries to branchless, truly digital banks [179][180]. In this context, the central role of bank branches has also eroded over the past decade.

New technologies and competition — banks now find themselves in competition not only with their peers, but with many new entrants (e.g. digital banking start-ups and fintech firms[17] or other non-bank digital corporations). This increase in competition leads to increase in customer expectation — customers will now expect new functionality and services to be available to them quickly, at any time and from anywhere [175][177][178][179].

This then leads to the following summary and short definition for digital banking:

> ***Digital banking*** describes the integration of digital technologies into the business model and overall organisation, including the provision of banking products and services through digital means and with a focus on customer experience. Furthermore, digital banking expands beyond banks and financial institutions: non-bank institutions (e.g. payment providers, credit card issuers, e-commerce and other digital corporations) are now part of the ecosystem.

2.5.2 The interplay of usability and security in digital banking

Elements of digital banking such as banks' websites with transactional functionality, dedicated mobile banking applications or various authentication mechanisms including passwords or token-based systems have been subject of academic studies over the past decades, continuously highlighting its special nature at the interface of usability and security. Digital money and 'financial interactions' have been identified as interesting starting points for HCI research, for example at the *#CHImoney* workshop[18], making use of the multidisciplinary toolkit of the area (computational and empirical methods paired with real-life applications [182]). Kaye et al. [183] have aimed to describe the "complexity and richness" of the subject of personal finance from a HCI perspective, with many mental tasks and decisions faced by users, requiring them to constantly balance their emotions around money, uncertainties, personal history and values as well as their (lack of) knowledge in regard to managing their own finances. Lewis & Perry [184] have continued and updated this enquiry in their qualitative study on personal finances in the UK from 2019, confirming the increasingly digital nature of personal finances and moving away from physical entities such as cheques or activities in branch. But in their view digital finance has also created new responsibilities and problem fields for users, e.g. socio-financial debt and money management within various social groups like partners, families, friends or colleagues, also challenging the narrative of digital finance and its related 'moneywork' (everyday interactional and social work around money [185]) as

[17] The term 'fintech' or 'FinTech' as a short form of 'financial technology' can be defined as "companies (or their representatives) that combine financial services with modern, innovative technologies" and "technologically enabled financial innovation. It is giving rise to new business models, applications, processes and products" [181]. Often, fintech companies will be looking to offer innovative products and services trying to solve direct customer or market needs, potentially giving them a competitive advantage over traditional financial services peers [180].

[18] *#CHImoney* was an event of workshop type format at CHI 2014, with the intention to bring together both researchers and practitioners interested in "social, technical, and economic aspects around everyday user interactions with money and emerging financial technologies and systems" [182]. CHI (ACM CHI Conference on Human Factors in Computing Systems) is one of the leading international conferences for the research area of HCI.

a more convenient and value-added alternative to traditional banking activities. While these works with their precise focus on digital personal finance only lightly touch on security and privacy aspects, the integral need to guard financial assets adds another layer of complexity for system designers and users [186], emphasising the important role human users play in protecting against attackers as their malicious counterparts.

Hertzum et al. [187] describe this "conflict between ease of use and security in the context of usable security" using the example of the digital banking facilities provided by six Danish banks as early as 2004: trade-offs between the two were encountered at various levels of these systems, ranging from individual features such as restrictive password rules or around the level of instruction provided to the user to enable them to complete complex security tasks. They argue the surveyed systems heavily relied on this 'instruction' type element of usable security approaches as a way to elevate usability levels. This is in contrast to 'automating' ease of use by simplifying the user interface or fostering 'understanding' of security processes and requirements in the user (the two other approaches in usable security put forward by Whitten & Tygar [188]). In their view, users may ultimately accept these limitations to ease of use to accommodate security requirements, without knowing too much about the exact workings of the protection measures in front of them [187] — Furnell [189] corroborates this view, expecting users to "typically be more tolerant of additional security measures than they would in other situations" to help protect their assets. But this acceptance level is likely to be finite as remarked by Weir et al. [50], requiring banks to carefully consider the balance between technical security levels to protect them from cybercrime losses and the willingness and capability of users to accept and adopt security measures [190][191]. Failure to acknowledge this principle of psychological acceptability (Bishop in Cranor & Garfinkel [192] ch.1) and accommodate human user needs (the 'human factor' in Adams & Sasse [193]) may lead to users completely avoiding system usage (or potentially adopt workaround solutions that may compromise security levels where available [50]). As expanded on by Pikkarainen et al. in their influential study on consumer acceptance of online banking [194], continued user preference of traditional, analogue channels such as branch visits may lead to loss of market share as users switch to competitors offering superior, ultimately more user-friendly, value-added solutions [179].

Owed to this challenge of balancing security and usability for users as well as business needs, banks have relied on a multitude of different security solutions and authentication mechanisms, with approaches changing over time to meet security needs and reduce cybercrime losses. Nilsson et al. [195] for example have compared differences in early approaches in the UK (fixed, same password used every time) and Sweden (one-time password, token-based solution) in their 2005 short study, concluding on how trust in online banking by users is influenced by security mechanisms as well as the situational settings (e.g. use of public computers). These approaches would differ considerably from for example German banks providing their customers with physical lists of one-time passwords or transaction numbers ("iTAN" in [196]; also in [50]). Kiljan et al. [197], Choubey & Choubey [198] and, recently in 2020, Sinigaglia et al. [199] have provided an extensive overview of authentication solution across the world, showing a wide range of proposals across different financial services organisations and geographical regions. While a definite lack of formal standardisation can

be observed here [198], most systems will however now rely on two-factor authentication[19], consisting of one or more passwords and usually a further one-time password delivered via a token or mobile phone, or even paper [50][196][199][200][201], although other solutions based on software certificates or biometric details exist, including Apple TouchID [197].

In an early effort to investigate user adoption of online banking amongst Finnish banking customers, Pikkarainen et al. [194] in 2004 suggested a model containing three new variables (security and privacy, enjoyment and available information) in addition to perceived usefulness and ease of use from the original 1989 technology acceptance model (TAM). Furnell [189] has suggested a number of assessment criteria in his comparison of password-based UK authentication approaches in 2007: these include required mental effort, convenience (e.g. speed) and flexibility for the user, but also applicability across a number of device types and settings as well as mutual authentication (where both the user and the bank are able to verify their identity accordingly). Additionally, Just & Aspinall [200] have described feedback as a usability property in this context, specifically timing and granularity.

Evaluating usability in practice, Weir et al. [50], in their full usability study, compared both single-factor authentication (two layers of passwords) and two-factor authentication (one-time passwords via a token; or via mobile phone delivery). The observed general user preference is divided relatively equal across all three methods — however, 10 years on from their study, a further shift towards mobile devices could be expected today. Furthermore, users seemed strongly influenced by habitual effects (Lichtenstein & Williamson in [50]), scoring both usability and security more positively in methods they regularly used, regardless of their theoretical security levels — accordingly, their willingness for adopting new and enhanced protection mechanisms was limited, hinting at a lack of understanding why this was necessary or beneficial to them. While this lab-based study used a relatively large sample (141 participants) and a survey study, it also relied on prototypes rather than live systems. Krol et al. [201] addressed this issue by using in-depth, semi-structured interviews and diary studies ('authentication diaries') to assess the usability of different two-factor authentication approaches in the UK in their study from 2015. Their findings led to recommendations to support user experience through consistent terminology across the industry (as many users would have accounts with more than one bank), to reduce the number of steps in the authentication process (also suggested in [202]) and ideally to remove 'inconvenient' physical tokens which created dissatisfaction in the study participants. This is also supported in Reese et al. who reported on one third of surveyed users not having their token with them at some point during the period of their observation study in [203].

While these studies highlighted central problems in the field, the sample was made up of relatively young, educated and technically savvy users, possibly not representing the larger general, varied population of digital banking users. Additionally, Krol et al. [201] hinted at the future potential of objective empirical data directly from banks (if this could be obtained) rather than using self-reported data (from a smaller sample). Recent studies such

[19]Two-factor authentication will rely on two elements to authenticate the user, e.g. knowledge (a secret, password or PIN), possession (a personal object like a bank card or trusted phone number) or biometric information (like a fingerprint) — this is in contract to single-factor authentication, which may only rely on one element (even if used multiple times) such as passwords (adopted from Weir et al. [50]).

as Zimmermann & Gerber [204] in 2020 have confirmed the correlation of perceived usability of authentication solutions, but not security or privacy, with user preferences, also suggesting to consider these discrepancies around user perception when deciding on the design of digital banking security solutions. Making these design decisions potentially even more difficult, Cristofaro et al. [205] suggest that usability perception in two-factor authentication solutions is strongly correlated with individual user characteristics such as age, gender or background rather than the technology itself (or its context of use) — with its wide-reaching user base, banks may struggle to design truly inclusive solutions that feel equally usable for all.

In practice, the complexity of authentication solutions and related usability implications remains high: to keep up with the evolving threat landscape, meet security best practice needs and comply with regulatory requirements [199][202]. Technical security solutions to secure digital banking channels have been continuously developed and updated to address latest cybercrime trends and reduce related losses over the last two decades [189][196][199]. However, the focus has also been on the human user as an attack surface targeted by cybercriminals. Mannan & Van Oorschot [191] have discussed key expectations towards users put forward by banks in relation to security, e.g. installation of anti-malware programmes, regular software updates and basic understanding of SSL certificates, also observing limited compliance levels in their survey study: 65% of participants (123 individuals recruited within a Canadian university department) stated that they did not read any banking agreements, whether caused by lack of knowledge, understanding or unwillingness. While this study now dates back to 2008, Becker et al. updated and extended this observation in their detailed international comparison on bank fraud reimbursement from 2017, where only 35% of participants stated they fully understood banking terms and conditions (from a heterogeneous sample of 151 paid participants in the UK, US and Germany) — this study also touches on the question of responsibility and a potential liability shift [20] from banks to customers.

Lastly, in addition to the technical authentication solutions and mandatory non-technical requirements as mentioned above, financial services institutions have also focussed on security education and training of their users as human elements that may become an attack surface. These efforts range from simple security advice on their website (e.g. 'Stay safe with Monzo' in the UK [210]) to dedicated, large-scale digital training and security awareness campaigns (e.g. Barclays in the UK and their 'Digital Eagles' programme [211]) or industry-wide initiatives (e.g. the 'Take five' campaign led by UK finance urging banking customers to adopt a mindset of 'stop (and think) – challenge – protect' in online settings [212]), with specific attempts to deter young people from being recruited as money mules also in existence (in the UK: [213]).

[20] The question around where liability for bank fraud losses falls between banks and customers remains complex: in principle, "where a customer hasn't authorised a payment, the bank should refund the money — so long as the customer hasn't acted fraudulently, or with intent or 'gross negligence'" (wording from UK Financial Ombudsman [206]). A problem can arise from the aspect of a valid, genuine authorisation — attackers may for example trick banking customers into authorising transactions to an account that appears legitimate but is controlled by the attacker without their knowledge ('authorised push payment scams' [207]). In the UK, a voluntary code of practice was proposed in 2019, to enhance efforts to protect and reimburse customers when the expected level of care was met on both sides ('no blame' scenario) — individual cases may however still not be covered under this proposal [206]. Filling this gap, individual banks have pledged to refund all transactional fraud losses, e.g. TSB UK: 'fraud refund guarantee' in 2019 [208]. However, the overall picture remains to a degree fragmented, with some banks not subscribing to the code [209].

These commercial perspectives correspond to a growing body of academic research concerned with the evaluation of security education and awareness approaches, also specifically for the case of phishing. Kirlappos & Sasse [214] have argued against too generic security training and awareness campaigns, proposing a move to context-specific training including a feedback loop to test newly acquired understanding and skills (e.g. to distinguish legitimate and fraudulent sites) — working and validated examples of such embedded, interactive training systems have been provided e.g. in Kumaraguru et al. [215] in their "School of phish", also including game-based approaches. And specifically to online banking, Jansen & Leukfeldt [216] suggest further experimental research into fostering a deeper understanding of threats and past attacks in users to raise awareness and ultimately also protection levels. While these proposals seem to potentially extend beyond many real-life examples of security education and training employed by banks (although the sophistication and complexity of these varies significantly as indicated above), Volkamer et al. confirm an overall positive effect on phishing awareness in users even from condensed training videos (five minutes in length) in their empirical study in [217], although assessing the quality and ultimate effectiveness of current educational offerings around security made by banks remains difficult at this point in time.

2.5.3 Digital banking attackers in literature

This section comments on the treatment of attackers specific to digital banking as found in previous literature. Crucially, at this point in time, the researcher is not aware of exact replications close to the studies undertaken in Chapters 6 and 7: i.e. no attacker categorisations such as taxonomies or typologies (in the sense of works as described in Section 2.3) specific to digital banking have been found in past literature, and similarly, the compact body of literature on attacker personas reviewed does not appear to include a banking-specific application. Nevertheless, attacker types and groups relevant to the context of digital banking have been described, ranging from general models to more specific, empirical analysis of certain actor types — these themes are discussed in the remainder of this section. Additionally, references to literature have been made directly in the results presentation in Chapters 4 and 5.

Actors in the context of digital banking have generally been described as embedded in the larger ecosystem of financial cybercrime[21], emphasising the networked nature and prevalence of groups (or at least loosely connected individuals), but also the high level of commercialisation, organisation, specialisation and division of labour in this context, e.g. in Kraemer-Mbula

[21] To define the term cybercrime specifically for the context of this thesis, the recent (2019) review on defining cybercrime by Payne in [218] has been consulted, considering the challenges around defining cybercrime (e.g. its global and multidisciplinary character, but also an apparent scarcity of criminological research in the area) as well as options for conceptualisation (e.g. as a traditional crime, deviant behaviour or technological problems amongst others). Additionally, while a distinction between 'cyber-enabled' crimes (traditional crimes enhanced in form, scale or reach through the use of IT systems, e.g. data theft or fraud [219]) and 'cyber-dependent' (the use of IT systems to commit new types of crime unique to electronic networks, using attack vectors such as e.g. DDoS or malware attacks [219]) is commonly made, Lusthaus [220] considers this debate as largely irrelevant in a sociological, non-legal context trying to understand human factors. Leukfeldt [92] has also distinguished between crimes where IT is both instrument and target or is only instrument, although both authors ultimately adopt a general, 'umbrella' term style definition. This broad approach is followed in this thesis, where cybercrime is understood as the use of IT to enable criminal activities, specifically in a financial services environment and targeting or affecting digital banking applications.

et al. [221], Sood et al. [222], Huang et al. [223] or in the works of Leukfeldt [92] or Lusthaus [220]. Nurse & Bada have supported this thinking by suggesting an evolution from individual attackers and small-scale attacks to group-based structures in [224] (although this work has only had a limited focus on financial services). Moore et al. [225] also observe this effect as an "industrialisation of online wickedness" in their 2009 work *The Economics of Online Crime* in the area of security economics.

While the term 'organised crime group'[22] has been readily adopted by some to represent the current threat actor landscape (e.g. in Choo [229]), questions have been raised as to whether such crimes even constitute organised crime [226][230]. Further to this, Lavorgna & Sergi [231] argue the juxtaposition of 'serious' and 'organised' when defining cybercrimes: while these crimes may be of serious nature, they are not always part of organised crime activity. Overall, conceptualising cybercrime as organised crime may be problematic: employed definitions may lack academic rigour [226] and the usage of the term may imply aspects not contained in current cybercrime structures (such as the assumed 'mafia' narrative criticised by Wall in [232]). Methodologically robust empirical evidence to confirm the organised crime elements in cybercrime groups seems limited at this point in time (e.g. in [226][230][231]).

Despite this, it is crucial to realise that business models for financial cybercrime show high levels of sophistication, organisation and overall complexity, with a multitude of activities and actors included in the overall process. At a general level and cited regularly in related literature (e.g. [45][224][228][230][233]), Choo & Smith [227] distinguish between three types of organised criminal groups: groups relying on IT to expand their traditional criminal activities such as fraud or data theft; groups operating exclusively online; and organised groups using IT for their ideologically and politically criminal activities. Business models such as crime-as-a-service as a way of purchasing specialised services ranging from the supply of customised malware, counter anti-virus services, hosting services, escrow or 'drop' services (where illicit gains are transformed and taken out as funds [234]) may add further technical capabilities to the skill portfolio of traditional criminal groups [221][224][235].

In their typology of group structures, McGuire in [233] (also referred to in [224][230]) describes traditional, organised ('hierarchies') as well as loosely organised ('aggregate') attacker groups using IT to enable and expand their criminal activities. In contrast to this, two types of groups mainly operating online are proposed by McGuire: disorganised 'swarms' of individuals united by a common (criminal) goal, but without a clear command structure, and organised 'hubs' of criminals organised around a group of core criminals — Broadhurst et al. [233] place phishing as a digital banking related activity in this category. Interestingly, 'hybrid' group structures, where attackers are able to transition efficiently between online and offline environments, are also considered in this context, with specialised clusters of attackers engaged in specific types of crime, e.g. credit card data theft and subsequent sales through underground channels (McGuire in [233] and Soudijn & Zegers [236]; also in Kraemer-Mbula et al. [221]).

[22] In this thesis, the suggested definition from Varese in Lusthaus [226] derived from Schelling's reasoning is adopted, where an organised crime group is understood "as one that attempts to regulate and control the production and distribution of a given commodity or service unlawfully". This governance-based approach supplements the more general definition focussing on group structure in Article 2 of the *UN Convention on Transnational Organized Crimes*, which is relied on by e.g. Choo & Smith [227] or Hutchings [228].

The NCSC in the UK [235] describes these attacker clusters further and provides a concise overview of specific roles incorporated in the business model underlying financial cybercrime. These roles may include crime organisers or team leaders, coders and malware developers, network administrators or bot herder (also in Moore et al. [225]: a function to manage, operate and rent out "a large collection of compromised personal computers"), intrusion specialists and data miners, but also money specialists to monetise the stolen assets. Previous to this, a similar list was also provided by Chabinsky at the FBI ([237]; also in Broadhurst et al. [233]) on typical specialisations in cybercrime, showcasing the wide range of skills and functions in existence in cybercrime organisations. While both of these lists originate from government institutions, no research design or data sources are described for these works to the knowledge of the researcher, hindering further verification, extension and comparison with other findings. However, it is worth noting that such proposals are likely informally grounded in observations and would form a realistic representation of the attacker landscape, in contrast to abstract attacker models: the work of Sinigaglia et al. [199] for example has introduced such an attacker set specific to digital banking authentication, consisting of entities such as device thief, shoulder surfer, eavesdropping software, social engineer, man-in-the-browser and man-in-the-mobile — these categories are likely to be closer aligned to attack vectors than to represent human attackers.

While the works mentioned so far in this section are certainly useful to understand the attackers and groups involved in cybercrime targeting digital banking specifically, their grounding in real-life data seems limited — only a small number of truly empirical works appear to exist for the specific context of digital banking. Hutching's qualitative analysis examining criminals engaged in computer crimes and fraud in Australia [228] includes a limited number of individuals involved in attacks against digital banking services, without providing further detail and overall aligning them with Choo & Smith's three attacker group types (with ideologically motivated attackers assumed to only play a minor role). Birk et al. have provided a practical model of phishing attacks, dividing relevant actors into technical functions, intermediaries or financial agents tasked with money transfers and withdrawals — while their findings are intriguing, their research [238] based on "close cooperation and information exchange with banks, lawyers and phishing victims in Germany" does not include exact data sources or research procedures.

Providing further empirical data for the specific context of digital banking, studies by Lusthaus and Leukfeldt respectively should also be considered. While Lusthaus has extensively written about profit-driven cybercrime, the fieldwork study *Offline and Local: The Hidden Face of Cybercrime* ([239], with Varese) on cybercrime organisations in Romania is of particular use to understand the current reality of financial cybercrime, observing a strong offline and local dimension to cybercrime operations (i.e. involved attackers would know each other personally and reside locally), strict division of labour and low level of violence. Leukfeldt's datasets in their extensive work on *Cybercriminal networks* in [92] are entirely specific to digital banking and derived from criminal investigation reports and interviews with investigators (for the Netherlands; although some data for Germany, the UK and US was collected for comparative value [92] p.99). Beyond discussing aspects around group structures, social ties and capabilities, three attacker types are synthesised from the data analysis in his research: core

members, enablers (e.g. suppliers of customised malware or bank employees to support the planned attack from the inside), and money mules [230].

Money mules have received particular attention as a group of actors in the context of financial cybercrime: these non-technical supporting actors are recruited and employed by organised crime groups and networks for the purpose of money laundering [235], disguising the origin of illicit funds and ultimately extracting them. While the modus operandi of money mule activities may vary, the general process involves a number of rapid transactions across different accounts owned by mules, followed by the 'cash out' (also in [240][92] p.81), where funds are withdrawn (via an ATM) by another member of the group or network [240][241][242]. Money mules would generally not form part of "the group of core offenders coordinating the illicit activities" [243], but receive a commission in return for their risk-taking (the value of 5% is suggested regularly, e.g. by Europol in [240]; also in [236]). Leukfeldt & Kleemans [243] criticise the lack of empirical research into this group of actors in the past, with limited data-backed case studies produced over the years (e.g. [236][244][245]).

Nevertheless, recruitment channels for money mules have been defined widely in literature, with both face-to-face recruitment, for example through existing social networks (e.g. from their own neighbourhood, school or sports club [243] or amongst families and friends [241]), but also virtual channels playing a role (e.g. through job adverts for work-at-home offers [225][244][246][247], direct emails [236], or social networks [241]). Individuals in the focus of mule recruiters may often display a level of vulnerability — in their in-depth analysis of hacker forums, Mikhaylov & Frank [248] showed examples of users discussing "students, drug addicts, homeless people and the elderly" as ideal targets (similarly in [243]). It is however also likely that specific requirements for mule activities strongly define the recruitment approaches, e.g. local language skills or access to specific digital bank accounts [245].

While an unsuspecting, unknowing nature of money mules, depicting them as victims rather than criminal actors, is suggested by some (e.g. in Cranor [247]), a complicity spectrum including unwitting, witting and complicit mules can be assumed as described by Raza et al. [241] (also in [249][246][225]). Leukfeldt & Kleemans have provided some empirical evidence from their analysis of 112 interrogations with money mules in the context of Dutch criminal investigations, stating that just over a quarter (30 individuals) felt that their actions were legitimate in [243]. Without further data, it remains difficult to confirm this exact role of money mules: however, money mule need to be considered as largely purposeful criminal actors in the overall business model [236].

We may not always completely understand why we and others do the things we do, but most times it makes sense. And when things make sense, you've made meaning.

— Johnny Saldaña,
"Researcher, Analyze Thyself",
keynote, 2018 [250]

3

Research Design

This chapter comprehensively presents the research design including all methods used within this thesis, starting with the definition of the theoretical lens and conceptual framework underlying this work. This is followed by a sequential overview of all research activities in this thesis and the statement of researcher positionality. Secondary, primary and additional data sources of this research are defined before setting out the exact research procedures for the data analysis presented in Part II and the three studies presented in Part III of this thesis.

The research design of a study defines all principle as well as further detailed methodological choices made and gives "specific direction for procedures in a research design" (Creswell [251] p.12). The aim of this chapter is to bring together all methodological aspects found in this project to prepare for the presentation of results in the remainder of this thesis — this is seen as beneficial due to the multi-part enquiry consisting of multiple, independent but strongly related studies contained within this thesis.

Directly continuing on from the background and literature review presented in the last chapter, this chapter sets out to provide a complete overview of the research design directing this project and is structured as follows: initially, the research paradigm and conceptual design underlying the research are detailed, explaining decisions made and placing the methods used into context with related existing literature. To help the reader understand the different parts or studies included, this is then followed by a sequential overview of all research activities,

including an infographic showing the order of and relationships between these activities. Further to that, the positionality of the researcher is defined at this point, helping the reader to understand how the researcher's person and background may have influenced this research design and the overall work. These sections are then followed by a detailed description of all data sources and procedures carried out for the multiple study parts, rounded off by a summary and outlook.

3.1 Theoretical lens and conceptual framework

Building directly on the literature review as well as research questions and objectives covered in the introduction, this section aims to explain the theoretical stance and the conceptual setting of this thesis. In addition to showing the general research paradigm underlying this thesis, this section specifically considers four major parts of theory: firstly, the choice of grounded theory as a methodological approach for the fundamental data analysis of attacker characteristics and behaviours is substantiated. This is followed by a note on how the research field of attacker taxonomies and typologies have influenced this thesis. Similarly, the understanding, adaptation and integration for the concept of attacker personas within this research are discussed. Lastly, relevant theory to attacker-centric thinking in security practice is defined, including its limitations (especially in the narrow context of financial services).

3.1.1 Philosophical paradigm

Philosophical worldviews or paradigms can be viewed as a "general philosophical orientation about the world and the nature of research that a researcher brings to a study" in Creswell ([251] p.6) or "a set of basic beliefs (or metaphysics)" in Guba & Lincoln [252]. Identifying the appropriate paradigm may "inform and guide enquiry" [252] as it formalises the hidden belief system of the researcher and may help to explain why a certain research strategy was chosen. The philosophical worldview held by the researcher can largely be described as constructivist, using an inductive research process aimed at theory generation and understanding in a social and historical context. Various data sources may present multiple perspectives and meanings — equally, the researcher's own experiences and background may shape interpretations of findings ([251] p.8/9 and Charmaz [253] p.14) as accounted for in the reflective positionality statement in the next section. There are certain elements of pragmatism present, defined by the orientation towards real-world practice given by the topic researched and the pluralistic element of the data collection and sources [251] pp.5. This pragmatic paradigm is mostly reflected in the intent of applying knowledge of attacker characteristics practically (or providing a set of recommendations to do so, as defined in Section 8.3.2).

3.1.2 Usage of grounded theory

To accommodate the principle enquiry into the nature of attackers targeting digital banking attempted in this thesis, an inductive qualitative research design has been chosen. Specifically, grounded theory analysis as a method has been adapted for the analysis of the large dataset

on cybercrime cases that helps to elicit the attacker characteristics and behaviours. Grounded theory is originally defined as "the discovery of theory from data — systematically obtained and analysed in social research" by Glaser & Strauss in 1967 in Urquhart [254] ch.1. In its original form, the focus of the method is on creation of theory that is profoundly grounded in data. Modern grounded theory[23] also emphasises the data analysis process: Charmaz ([253] p.1) accordingly describes its methods as consisting of "systematic, yet flexible guidelines for collecting and analysing qualitative data to construct theories from the data themselves".

From a methodological point of view, grounded theory was chosen to fit the subject of investigation and research questions: for this new area of enquiry (no dominant theories describing or categorising digital banking attackers specifically were found by the researcher to date as discussed in Section 2.2), grounded theory with its focus on working closely with the data and thorough iterative coding process with the intention of developing categories as well as ultimately concepts and theories seemed well suited [255].

This decision was guided by the pragmatic synthesis[24] of core grounded theory principles from key text and theorists by Timonen et al. [256]:

- Firstly, grounded theory should focus on absolute grounding in the data, with researchers looking for new aspects and facts in the data itself rather than testing hypotheses. This condition is met for the intended research as characterisations of digital banking attackers are limited in literature to this point.
- It should then capture and explain "context-related processes and phenomena" — this can be accommodated through various methods of data collection methods, as long as importance is given to the context in which these sources were created. Timonen et al. [256] see qualitative interviewing as most common, but also acknowledge documents as a valid source — the usage of secondary data within this research is discussed further below.
- Direct, deep engagement with data (including reflective memo writing) and constant comparison (continuously comparing data to data) was also directly relevant to this research: the intention of this research was to not only understand the nature of attackers, but also to define the categories of characteristics and behaviours that can be found in open source materials to best describe them.
- Lastly, theoretical sampling is used to shift analysis onto specific aspects and subsets in the data, to add further detail to categories and identify relationships between them. This approach is used throughout the data analysis to strengthen individual categories as presented in Chapters 4 and 5, but also through re-coding of the original dataset to prepare the attacker typology shown in Chapter 6.

Helpfully at this point, Hood [257] points out key differences between a generic inductive

[23] An in-depth discussion on grounded theory as a methodology, including its legacy, debates, differing interpretations as well as comprehensive reflections on the current status of grounded theory methods is provided in Charmaz [253] ch.12.

[24] In [256], Timonen et al. produced a compact, but comprehensive and accessible guideline to grounded theory and its challenges across major theorists and key texts, from early efforts by Glasser & Strauss and Strauss & Corbin to Bryant, Charmaz and Clarke as authors also mentioned in this section.

qualitative model of research (using the example of Maxwell, 2005 in [257]) and grounded theory as "theoretical sampling, constant comparison of data to theoretical categories and focus on the development of theory via theoretical saturation of categories rather than substantial verifiable findings" — these aspects and their integration in this thesis are shown in Table 3.1. It is worth mentioning that several other methods were considered, for example Clarke's situational analysis [258]. While Clarke's approach as an adaptation of grounded theory which considers all aspects of research context and situation through the use of cartographic analysis and visual mapping (e.g. through situational maps showing major human, non-human or discursive elements in the research situation and their relationships — refer to Clarke [258] p.366) is interesting, the situation of anonymous attackers was deemed too unclear to produce sufficient visualisations at the time[25]. Initially, Thomas' general inductive approach was also considered as a simple, non-technical set of data analysis procedures as presented in [259] — however, as grounded theory inherently included such procedures it was seen to offer additional benefits (compare to Table 3.1 for how these key characteristics of grounded theory have been treated within this research) and link in with related works.

The choice for using grounded theory was also influenced considerably by others using this method in the area of usable security, for example the works on attacker personas by Faily & Fléchais (e.g. on grounding personas through personas cases in [166] where grounded theory is used to explore attacker categories; also in Atzeni et al. [7]), but also older key works such as *Users are not the enemy* by Adams and Sasse from 1999 [260]. Similarly, grounded theory has been adopted widely in the context of HCI as an academic research field — this has for example been acknowledged in [261], in a panel discussion on second-wave theories in the field of HCI ('post-cognitivist') or in the insightful reflection on grounded theory use within the context of HCI postgraduate research in Furniss et al. [262]. Key works covering research methods specific to HCI have also included grounded theory in its canon of methods, e.g. Adams et al. [263]. Interestingly, grounded theory has also found entry into commercial HCI/UX research, e.g. underlying the creation of user personas at Spotify [264]. As the researcher has a professional interest in the area of human-centred design and HCI (refer to Section 3.3 on positionality), this relative prevalence of the method has potentially also influenced the decision to consider grounded theory for her thesis.

It is worth noting that this research uses an adapted version of grounded theory, through the usage of a finite dataset of secondary data (public information on cybercrime cases, mainly in the form of media articles as defined in Section 3.4). This method can therefore be conceptually aligned with Willig's abbreviated version of grounded theory [265]. Willig's understanding of grounded theory prescribes that only the original, predefined dataset is used (rather than the researcher broadening their analysis and adding further data as they move through the data analysis process). While all data is still analysed following the principles of grounded theory (e.g. constant comparison), other aspects such as theoretical saturation are

[25]Using the example of Friese's work on situational analysis, Clarke [258] argues against this: "However, I found the concept of the situation to be fully flexible enough to allow for the analysis [...] of tenuous and uncertain contemporary situations". This could be a future extension to this work based on the existing analysis — an example of a rich picture that was created as a memo that could serve as a starting point for this is included in Section 3.8.

confined by the finite dataset (refer to [265] p.39) — while this is not ideal (Willig remarks that "the abbreviated version of grounded theory should never be first choice), this variant is seen as beneficial to this research project due to its natural limitation in scope as a doctoral thesis. A similar pragmatic decision is for example defended by Hollywell [266] p.55 in their thesis in a healthcare and psychology context.

Additionally, while the usage of secondary data is not uncommon in grounded theory, it nevertheless poses challenges. Charmaz has discussed usage of secondary data and documents (either as elicited documents where research participants are involved in their creation or as extant documents where the researcher has no influence on these externally created assets) at length in [253] pp.45, also mentioning media articles as extant documents as relied on in this work [253] p.52. Quality of secondary data sources, data fit, lack of ability for theoretical sampling through additional data collection (e.g. follow-up interviews) and limited information on the context in which the original document was created (and how it can be viewed now) are all potential drawbacks to using secondary data in grounded theory analysis (in: Whiteside et al. [267], Andrews et al. [268] and Charmaz [253]). To address these issues, the data analysis procedures (Section 3.5.1) included an initial manual review and selection of documents from the original larger dataset, filtering out documents for quality issues or lack of relevance where possible. While further active questioning to accommodate theoretical sampling via participant feedback or adding new sources is not possible when using a finite number of documents in a pre-defined dataset, the large number of analysed documents paired with line-by-line analysis help to mitigate this limitation (Willig in [266] p.55; also in [267]. Lastly, the problem of context is probably the most difficult to address, given that the documents used originate from a multitude of sources such as media outlets or authorities. They will reflect, to varying degrees and either clearly visible or deeply hidden, the background, set of values and intention of the authors or organisations they represent. While this is hard to overcome, this research project may benefit from its narrow focus: information on individuals involved in cybercrime is usually fact-based (rather than on opinions or beliefs), e.g. directly from police reports or court cases. Additionally, the guide to critically assess documents in this context provided by Charmaz ([253] p.53) was considered helpful by the researcher. These issues and related adaptations to grounded theory in this work are included in Table 3.1.

From a practical perspective, the works of Charmaz [253] and Urquhart [254] (supplemented by Taber [269], Creswell [251], Willig [265], Bryant & Charmaz [270] and Timonen [256]) were mostly used as a guide for grounded theory aspects in this work. Also, like other data analysis methods, grounded theory places emphasis on the process of 'coding'[26] throughout the analysis stage ([253] pp.109–116). This research follows the guidance from Saldaña [271] on coding techniques specifically relevant to grounded theory studies (refer to Section 3.5.1 for full details on the coding processes).

[26]Coding can be understood as an analytical process where the researcher effectively 'tags' excerpts from the source materials with codes that have emerged from the data, with the aim of later grouping these codes together and developing categories from the data. Saldaña defines codes in qualitative enquiry as "most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data" [271] p.3.

Delayed literature review and theoretical sensitivity	While Charmaz ([253] pp.28) suggests an initial literature review, Glaser & Holton [170] see an extensive review before the identification of a core category as a violation of grounded theory principles. However, Glaser [272] acknowledges that wide reading enhances theoretical sensitivity — Thornberg (in [253] p.306) advocates an 'informed grounded theory' based on a critical reflection on related literature prior or during the research process. A literature review in close relation to the research questions has therefore been included in Section 2.5, carried out before the analysis process, but also adapted continuously during the process and for final presentation.
Emergent design and 'emergence'	Emergent design defines the research process as iterative, where only the initial stages can be planned in detail (in Taber [273] and [269]). Data collection and analysis may change or shift after the research has begun, based on what is learned throughout the process by the researcher (Creswell [251] p.186). Additionally, the concept of emergence as one of the key tenets of Glaser's thinking prescribes that theory is 'allowed' to emerge from data (in Urquhart [254] p.192). In this study, this is accommodated where possible: where indicated by emerging patterns in the data, materials were reviewed again and re-coded, facilitating deeper analysis to help build theory.
Theoretical sampling	In direct relation to the last point, the process of further data collection based on emerging concepts to develop, refine and test initial categories, their properties and boundaries. Tentative answers and concepts that have begun to form throughout the data analysis are verified to support theory development (Taber [269][273]; Urquhart [254] p.194; Charmaz [253] p.193, 344). This approach has been followed throughout the analysis by re-coding the large dataset numerous times to strengthen the initial categories. No additional sources outside of the original dataset were used for the analysis process, although references to related literature are added in the results section in Chapters 4 and 5. Additionally, the persona narratives in Appendix A for Chapter 7 have used several additional references to help tell their stories.
Constant comparison	Analysis follows an inductive process of comparing data with data/codes/category/concept — the analytical scheme is continuously being developed and checked back against previous data tranches and facets. In this study, data collection, transcription, coding and further analysis were conducted simultaneously where possible to accommodate this principle. The coding process following this principle is described in further detail in Section 3.5.1.
Theoretical saturation	"The point in category development at which no new properties, dimensions, or relationships emerge during analysis" about the emerging grounded theory (in Strauss & Corbin [274] p.143, also in Taber [269][273]). In this research, this is signified by "mounting instances of the same codes, but no new ones" in Urquhart [254] p.194. A level of validation for the level of theoretical saturation reached is also provided by a comparison to prior literature and its categories (as included in Chapters 4 and 5). Where categories and aspects have not reached significant levels of theoretical saturation, they remain tentative and are marked as such, e.g. within the typology in Chapter 6.

Table 3.1: ***Grounded theory characteristics in this research***

3.1.3 Further conceptual decisions and theories

The results from the grounded theory-based data analysis as presented in Chapters 4 and 5 are referenced further in subsequent studies, namely to construct a categorisation of attackers (typology) and attacker personas (as presented in Chapters 6 and 7). Additionally, an enquiry into how such strategies and attacker-centric security in general is used by security, risk and fraud professionals is presented in Chapter 7. While the sequencing and relationship between all these parts of the project is explained in further detail in the next section (Section 3.2), theoretical aspects shaping the conceptual framework for the later parts of this thesis are commented on below.

A critical reflective stance is taken to build our typology specific to digital banking. While the original intention was to reproduce earlier categorisation efforts and theoretically place this new typology alongside existing taxonomies and typologies (e.g. Rogers [23], Meyers [42], Hald & Pedersen [24] and Seebruck [25]), a more critical tone developed during the research process as many prior works seemed to show major methodological issues including a lack of transparency in regard to data sources used or in regard to certain visualisations used (circumplex presentations, e.g. in Rogers [23]). As discussed in the earlier literature review, this has also been acknowledged by De Bruijne et al. [26] and included in two publications of the researcher as [275][276]. In response to this, while this typology is firmly based on existing taxonomies and typologies, it uses a new, fully documented method utilising earlier results from the grounded theory analysis and affinity diagramming as a visual method to structure the attacker characteristics and behaviours into groups (as described in Section 3.5.2).

Building directly on the attacker typology, this work also produces a full set of attacker personas specific to digital banking in Chapter 7. While personas are usually applied to non-malicious users in a user research context, the theoretical grounding for personas outside of this context has been discussed before, e.g. in Bødker & Klokmose on 'techsonas' to represent technological ideas and artefacts [277]. Aucsmith in [6], Steele & Jia [44], Atzeni et al. [7], Tariq et al. [45], Faily & Fléchais [27] and Ki-Aries & Faily [167] have all described the use of personas in a security context as 'attacker personas' in the past (as referenced in Section 2.4). However, while these key works have promoted the concept of attacker personas and are relied on in this work, they do not present a full set of attacker personas together with their underlying creation method in all detail — they often focus on the context these personas are employed in, e.g. Ki-Aries & Faily [167], where personas are assessed for their value for raising security awareness. Although Aucsmith ([6] p.481) include persona cards and Atzeni et al. [7] define methodological aspects of their proposed persona development process, the limited presentation style may hinder the practical uptake of attacker personas or at least create quality issues in potential replication efforts. Additionally, the persona method can be classed as relatively mature in the area of HCI/UX dating back to the 2000s (Cooper [157][278], Grudin & Pruitt [279] and Nielsen [29][30]) and is now in use across a variety of commercial settings, with related documentation for their creation widely available. This work picks up on these two aspects and aims to show attacker persona creation based on Nielsen's 10-step process [29][30] borrowed from HCI. This approach supplements prior works rather than contradicting or criticising them, but it also enables questioning of the

perceived value of attacker personas in a professional setting (through a financial services survey as explained in Section 3.5.3) to help expand the research field.

The exploration of attacker-centric security with financial services professionals in Chapter 8 is principally grounded in the area of threat modelling, where the term 'attacker-centric' has been coined to describe an attacker focussed approach to security ('think like an attacker' in contrast to asset-centric or system/software-centric, e.g. in the key works by Swiderski & Snyder [102] or later by Shostack [6]). This enquiry was initially sparked by Shostack's [6] acknowledgement of the inherent difficulties with attacker-centric threat modelling, such as problems of accurate reproducibility, lack of structure to enable effective threat modelling and risk of introducing personal bias (as discussed in Section 2.2). As the theoretical grounding and available literature in this field are limited[27] at this point in time, a systematic literature review (following the example presented by Tuma et al. [62] in their work on threat analysis of software systems) was carried out to establish a status quo for this research field — this is included in the background to this thesis in Section 2.1.

3.2 Sequencing of research activities

Several studies are contained within this research project and thesis — while these can be viewed independently and have been published separately (refer to p.xiii), they are interlinked and partially build on each other in a sequential manner. To help the reader understand this sequence, relationships and dependencies between the different parts of this thesis, this short section describes the order of the research activities in more detail — Figure 3.1 helps to visualise this structure. A note on how and where these results are presented within this thesis is also made in the summary of this chapter in Section 3.6.

1. *Data analysis: characteristics and behaviours of digital banking attackers* — to establish the nature of attackers targeting digital banking services and systems in the best way possible, a large data analysis of secondary sources is carried out with the aim of describing their characteristics and behaviours displayed. While this research can be viewed independently, its findings also directly inform the following chapters, namely the attacker typology which is built through further data analysis and a clustering exercise. The attacker personas also rely on this data, indirectly through the typology which they build on, but also in the persona biographies and narratives (Appendix A).

2. *Study: typology of digital banking attackers* — using the results from the data analysis, this part builds out a categorisation of attackers relevant to digital banking grouped by common characteristics and behaviours as found in the dataset (a typology). Apart from the dependency on the initial data analysis, this study can again be viewed independently (and has been published as such by the researcher in [275][276]). However, in this research work, the following attacker personas study uses the finished typology as an initial outline for the attacker personas set to be worked on.

[27] Certainly in an academic context, although Adam Shostack runs a lively blog discussing the matter of attacker-centric threat modelling and security with supporters or critics of the approach, e.g. under [5].

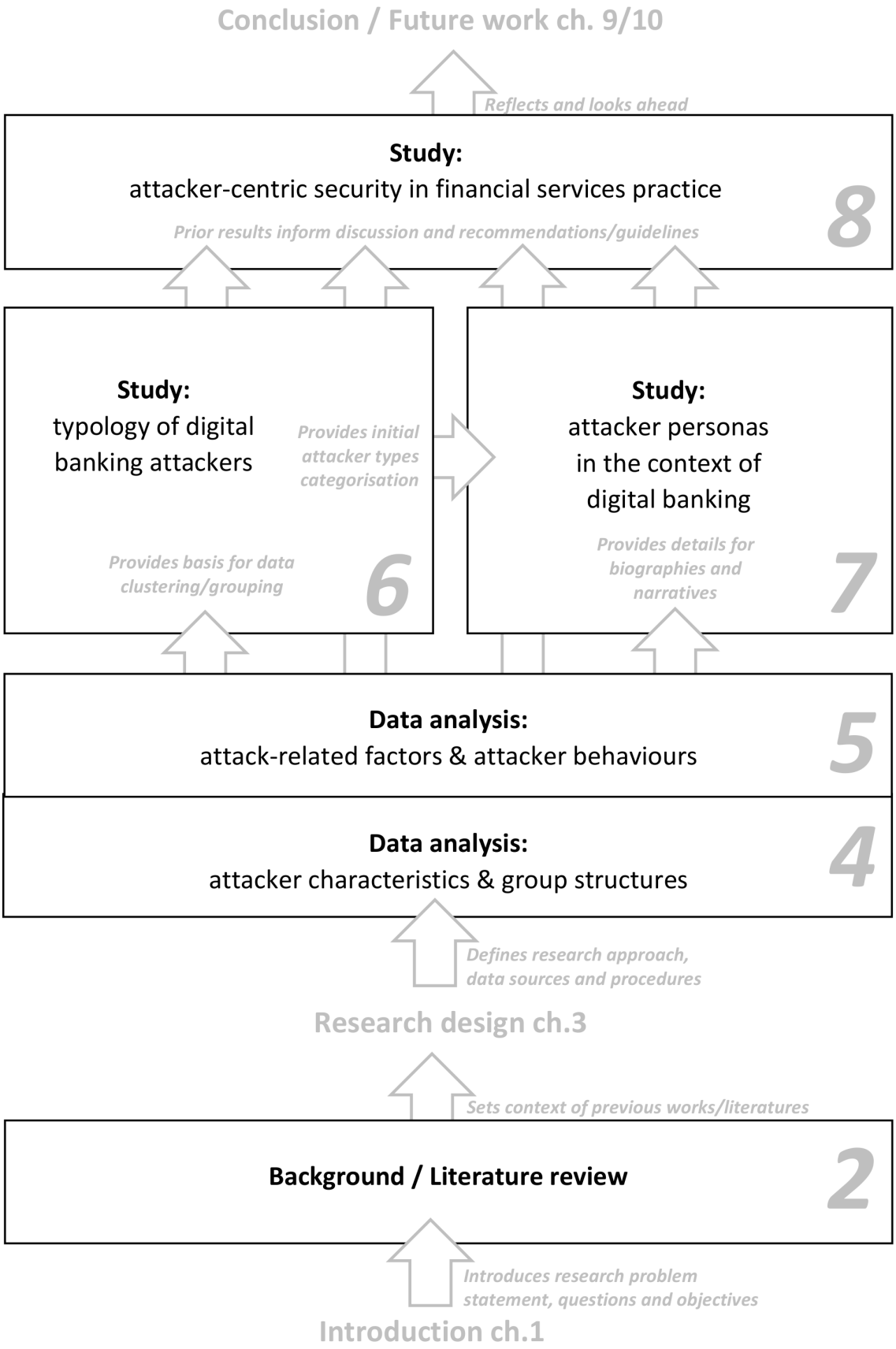


Figure 3.1: ***Overview of sequencing of research activities in this work***

3. *Study: attacker personas in the context of digital banking* — initially using the typology as a draft for the attacker persona set, the first part of this study sets out to extend the formal grouping and categorisation of attackers into detailed human archetypes (personas). As already mentioned, data snippets from the original dataset described in the last point are used for adding realistic details to the personas. Again, this part of the study has been independently published by the researcher as [280] and [281]. The second part of this study then places the attacker persona set in front of a professional financial services audience via a survey.

4. *Study: attacker-centric security in financial services practice* — the last research study was conducted with the intention of pulling together all prior results in this thesis and bringing them to the attention of senior financial services professionals in the form of an open discussion around how these financial services elites view attackers (and their human side) in their everyday work, leading to a list of recommendations for attacker-centric security. While this part of the thesis is largely independent (methodological aspects have been analysed and made available by the researcher in a workshop paper [282]), all prior learnings are seen to have prepared the researcher for holding these conversations, but also enable a critical reflection of new findings against the results from prior chapters. It can be said that this part of the thesis is deliberately set up to 'open up', also connecting academia and industry and generating some new research directions.

3.3 Positionality of the researcher

This section summarises important aspects of positionality and reflexivity for the researcher, including a brief note on the background of the researcher, but also the origin and major influences of this research project: the early beginnings of the 'research journey'. To understand and explain the concept of positionality, the (widely referred to) definition of Mullings [283] is relied on, which sees the researcher's "perspective shaped by his/her unique mix of race, class, gender, nationality, sexuality and other identifiers", but also the notes the "location in time and space" as a limiting influence on the researcher's knowledge, general view and interpretation of the world (also in [283]). It is also acknowledged that the researcher's positionality may have adapted throughout the research process, but may also vary for different parts of this thesis as a larger research piece consisting of multiple studies. For the interview study with elites working in financial services carried out in Chapter 8, a separate note on the positionality of the researcher specific to the interviewees and case organisation (insider versus outsider [283]; also in Lønsmann [284]) is made in Section 3.5.4. For the purpose of this research, 'other identifiers' as mentioned by Mullings [283] are most significant, with demographic and personal characteristics playing a subordinate (but relevant) role. Identifiers to be considered here are professional experience (including exposure to the industry examined), research experience and training/education.

The researcher has been working in retail banking across Europe for over a decade, in various roles in a digital context covering many aspects of usability and security as a designer and manager. She therefore has profound knowledge of retail banking, the related customer

perspective and internal product design processes (including how security is treated within interdisciplinary agile project teams). It is however worthwhile pointing out that she has not worked in a dedicated security, risk or fraud role to date (but has collaborated extensively with employees in these functional areas). While her academic training and education crosses the fields of digital design including HCI, business studies and information security, she also has extensive professional experience and training in the area of UX and human-centred design and research. This includes running design workshops, observing user testing, analysing user statistics or building prototypes. In summary, the researcher is very familiar with human-centred design aspects (including user profiling and personas) as well as retail banking as an industry, whereas knowledge on attacker profiling stems from this research rather than professional experience.

The demographic and personal background of the researcher is also likely to shape her research perspective to an extent when analysing the documents describing various cybercrime cases and attackers. The researcher is based in the UK and in full-time employment (in addition to fitting the WEIRD[28] acronym), which is in stark contrast to some of the individuals described in the cybercrime case studies (although some attackers will in fact come from a similar professional background to the researcher). While this has to be accepted, working closely with all the data available without employing subjective selection criteria (also refer to Section 3.4.1) and using grounded theory analysis can be seen to help balance this potential bias and to build a certain level of empathy or understanding for the human attackers involved.

It may also be helpful to understand the beginnings and major influences to this research project. For the researcher, the principle interest in information security and usable security in particular at an academic level initially arose from a comparative review of online banking security and its usability at a European level — the large variation across of methods used across European banking institutions sparked the interest of the researcher (as discussed in Section 2.5; also in her publications [53] and [286] previous to work presented in this thesis). In addition to this, the researcher's professional background and interest in human-centred design have certainly influenced the decision to focus specifically on the 'human element' of attacks. Lastly, it is worth understanding that this project also draws on the past work of the researcher [10][110] in the area of threat modelling as a professional and academic approach used in information security to identify, enumerate and classify threats and countermeasures to a system. Here, the early works on threat modelling and writing secure code from Microsoft (specifically Swiderski & Snyder [102] and Howard & LeBlanc [2]) have been of interest, as well as the works of Shostack [6] including the discussion of attacker-centric threat modelling have been a great inspiration for the direction of this thesis.

No direct funding has been received for this research project. However, it has been indirectly supported by a number of financial services institutions the researcher has worked for — for example through helping with participant recruitment, enabling her to attend academic conferences and providing relevant training.

[28] WEIRD: used to describe Western, Educated, Industrialized, Rich, and Democratic societies and its members in the context of social sciences or anthropology, mainly to acknowledge the sample bias found in many comparative social and behavioural science studies due to reliance on WEIRD samples rather than the wider population (in Henrich et al. [285]).

Ch.	Research activity	Data source	High-level rationale
4/5	Data analysis of attacker characteristics and behaviours	Secondary data sources (explained in Section 3.4.1)	Exploration and description of attacker characteristics and characteristics grounded in real-world data on a large number of cybercrime cases
6	Attacker typology build	Secondary data sources (Section 3.4.1)	Build an attacker typology based on attacker characteristics and behaviours from real-world data
7	Attacker personas build	Secondary data sources (Section 3.4.1)	Create a set of attacker personas based on an attacker typology from real-world data
	Attacker personas — validation and analysis of perception amongst professionals	Primary data sources (Section 3.4.2): survey study (Section 3.5.3)	Test and gather feedback on the personas created specifically and attacker personas in general
	Attacker personas — narrative stories	Additional data sources (Section 3.4.3)	Write compelling, but realistic narrative stories around the attacker personas created as a supplement to the personas
8	Attacker-centric security — exploration of thinking patterns amongst financial services elites	Primary data sources (Section 3.4.2): interviews (Section 3.5.4)	Explore how senior managers in risk, security and fraud working in financial services use and think about adversarial elements in their daily routines and professional environment

Table 3.2: ***Overview of data sources as used within this thesis***

3.4 Data sources

This section presents an overview of the data sources used throughout this thesis: this includes secondary data from four different sources in the form of publicly available information (web links/articles) on attackers and cybercrime related to digital banking. Secondly, primary data sources created by the researcher through the means of survey and interview studies are used within this thesis. Lastly, a small number of additional resources (web links/articles) have been added where deemed useful (in support of the narrative stories for the attacker personas as shown in Appendix A). Table 3.2 provides an overview to the reader on where these data sources have been used within the thesis and how they have informed research activities (directly or indirectly).

3.4.1 Secondary data sources

As already indicated in the conceptual framework and sequencing of research activities in Section 3.2, the analysis of a large number of secondary sources in the form of web links/articles plays a central role in this thesis. While an enquiry using primary data (for example derived through interviews or a survey-type study with security experts in financial services) was considered, two aspects influenced the decision to use secondary data: firstly, the intention was to provide an all-compassing overview of the attacker landscape independent from in-

Title	Geography	Timeframe	Items	Reference
BCS Cybercrime Forensics Specialist Group Briefings	Worldwide	2010–2014	487 lists with 7305 document links (127 relevant)	[35] and Appendix B
Cambridge Computer Crime Database	UK	2010–current	689 (90)	[34] and Appendix B
FBI Cyber's Most Wanted	Worldwide, subject to US prosecution	Current	43 (32)	[36] and Appendix B
Vocabulary for Event Recording and Incident Sharing (VERIS)	Worldwide, US focus	2012–current	7833 with 688 related to the finance/insurance industry (78 directly relevant)	[37] and Appendix B

Table 3.3: ***Overview of secondary data sources as used within this thesis***

dividual banking institutions (which may have specific threat profiles) — there was also a practical component for choosing this focus: recruitment of participants across different institutions proved difficult for the researcher[29]. Secondly, the datasets available were deemed as interesting starting points from reputable sources (e.g. University of Cambridge, VERIS), helping to showcase the potential benefit of using such sources for building human attacker profiles (possibly in the context of threat intelligence).

Four open-source datasets were ultimately chosen based on their public availability, scope and quality standards[30] — the researcher is not aware of an alternative larger datasets fulfilling the purpose of this research, but other sources (possibly restricted for public use) are likely to exist and would enable a replication of this study at a later point. The four individual datasets analysed are shown in Table 3.3 for overview and then described in full detail in the remainder of this section. A number of word cloud representations were created to visualise the content of the articles contained in these datasets (an overview of the most commonly occurring words across all datasets is shown in Figure 3.2), but also to show the difference between the four datasets (Figures 3.3 to 3.6).

[29] About 20 financial institutions, including financial services start-ups amd challenger banks, were contacted in regards to this research; with all of them, if they were not approached through one of the researcher's personal contacts, not willing to participate — while this may simply have been due to the student status of the researcher rather than being a member of a larger funded research group, the affiliation with another UK financial institution and competitor may have also played a role. This limitation also applied to the recruitment for the interviews as outlined in Section 3.5.4.

[30] The individual sources contained in these datasets are derived from global media outlets and police reports. While the data extracted is of largely factual nature (e.g. age of attackers), the documents were carefully reviewed (and removed) for a potential bias using Charmaz' guidance on studying, questioning and 'situating documents in their context' [253] pp.52. While a level of validation using additional (primary) data sources is carried out later in this thesis to also help offset any unwanted biases, further validation (also including new data) is strongly recommended in the future to help build a realistic and valid view.

Figure 3.2: ***Visualisation of word frequency for all datasets***

BCS Cybercrime Forensics Specialist Group Briefings

Firstly, a large collection of documents was sourced from the weekly cybercrime briefings of the British Computer Society (BCS) Cybercrime Forensics Specialist Group, compiled and published to the membership of the group by Denis Edgar-Nevill from 2010 to 2014 [35]. There were about 500 briefings overall, each containing up to 25 links to web articles and documents describing cybercrime cases of all types. About 130 of these documents were classed as suitable in an initial review of the source materials (refer also to Section 3.5.1) and relevant to banking-related cybercrime attacks. These articles and documents were derived from worldwide English language news outlets, ranging from government news channels, local and national newspapers to special interest online magazines or websites. Selection was made by the original author, aiming to represent cybercrime cases from countries around the world and to keep up with current developments in a fast-changing and developing area [35].

Figure 3.3: ***Visualisation of word frequency (BCS dataset)***

Cambridge Computer Crime Database (CCDB)

The BCS briefings ended at the end of 2014 when Edgar-Nevill retired [35]. To continue the work in a similar fashion, an adequate data source was found in the Cambridge Computer Crime Database made available under a creative commons attribution licence and continuously updated by Alice Hutchings at Cambridge University [34]. At the point of finishing data analysis (March 2020), 680 case notes on cybercrime offenders were included from this database. 90 documents contained information on banking-related cybercrime attacks and were deemed suitable in an initial review of the source materials (refer also to Section 3.5.1). While the nature of the individual documents is similar to the BCS materials and the coverage of the Cambridge database also starts in 2010, there are several differences. The Cambridge database focuses on the United Kingdom, while the BCS briefings cover a global spectrum. These briefings also report on cases as they happen, while the Cambridge database only includes a case once the "offender has been arrested, charged and/or prosecuted" [34].

Figure 3.4: ***Visualisation of word frequency (CCDB dataset)***

FBI Cybercrime Most Wanted

A third source was used to add further potential for comparison and verification of emerging patterns during analysis. The Federal Bureau of Investigation (FBI) produces a Cyber's Most Wanted list [36] in addition to their 'most wanted' list for any criminals or group of criminals engaging in cybercrime of all types. These 43 profiles of cybercriminals have been added as sources, however only 32 of them are relevant to digital banking in a wider sense and were deemed suitable in an initial review of the source materials (refer also to Section 3.5.1). This source not only differs in amount of case documents included, but also shows a different structure: rather than linking to articles or documents from external sources, the FBI lists present short profiles of cybercriminals together with an appeal for submitting information regarding the individual criminal. The FBI list covers a global range of high-profile cases; however, all criminals are naturally subject to prosecution in the US.

Figure 3.5: ***Visualisation of word frequency (FBI dataset)***

VERIS Community Database

Lastly, another current, large scale data source in line with the BCS and Cambridge Computer Crime Database datasets consisting of a list of web links to cybercrime cases is added: the VERIS Community Database [37]. VERIS is owned and developed by Verizon[31] and stands for the Vocabulary for Event Recording and Incident Sharing schema, a structured approach for recording and sharing real-world attacks through a set of variables to describe them as accurately as possible. As VERIS aims to address the lack of an "unrestricted, comprehensive raw dataset available for download on security incidents that is sufficiently rich to support both community research and corporate decision-making" [288], the latest dataset is available for download through GitHub [37]. The database version (October 2019) used within this thesis contains a total number of 7833 incidents, with 688 related to financial institutions in the widest sense[32] — 78 of cases were subsequently deemed as suitable. While the VERIS dataset contains information similar to the BCS and Cambridge datasets (namely links to web documents for further content analysis), its precisely structured export format (e.g. as an Excel sheet) supports initial analysis greatly. It is worth noting that the database can be contributed to by community members via GitHub, although coding standards need to be maintained and basic quality checks ('sense checking') are in place through other community members. While the database includes cases from all over the world, a US focus can be observed (potentially due to the location and expertise of the contributors).

[31] Verizon originally created and own VERIS as a structured schema for incident data recording. The framework is also used within the creation of their annual Data Breach Investigations Report [287], which is considered a key industry resource on data breach information and statistics. The raw data used to create the report is however mostly restricted and not available to researchers, which led Verizon to the launch of the VERIS Community Database as an initiative to make incident data available to the wider security community [288].

[32] VERIS uses the North American Industry Classification System (NAICS) to identify the industry affected for the individual case. While the sector code '52' classifies 'finance and insurance', the case number for cases related to digital banking in the dataset is significantly lower — as no adequate filtering mechanism was available, manual analysis by the researcher had to be carried out as described in Section 3.5.1.

Figure 3.6: ***Visualisation of word frequency (VERIS dataset)***

3.4.2 Primary data sources

While the analysis of secondary data sources plays a central role within this thesis, there are also two sets of primary data created for this research: firstly, quantitative and qualitative data through a survey study on the perception of attacker personas amongst financial services professionals and secondly, qualitative data through in-depth interviews with senior managers in a financial services institution investigating their patterns of thinking around adversaries and attackers. A brief summary of these two data sources is presented below to help provide an overview of all data sources used within this thesis in one place — full details on these studies is provided in the research procedures in Section 3.5.3 and 3.5.4.

Survey study: perception of attacker personas
To support the validation of the attacker personas created within this thesis and as part of the overall conceptual framework, a survey amongst financial services professionals asking them about their perception of the attacker personas was created in this thesis (Chapter 7). An online questionnaire consisting of 32 Likert-type questions loosely based on the 'personas perception scale' framework by Salminen et al. [289] (investigating attitudes towards attacker personas in regards to factors such as clarity, completeness and consistency, credibility and empathy, relevance and applicability as well as usefulness and willingness to use) was sent out to over 1,000 financial services professionals, resulting in 85 full responses.

Descriptive analysis was conducted using the quantitative data derived (e.g. mean/median of values across the sample — due to the limited sample size, no further statistical analysis was carried out). Qualitative data collected was analysed using basic descriptive coding. An overview of these results was then added to Chapter 7 after the presentation of the attacker personas in question, showing the potential, but also issues that practitioners saw in these personas specifically and the tool in general. Exact information on the data collection and analysis process including information on the adopted framework by Salminen et al. [289], structure of the questionnaire, recruitment and the statistical analysis processes are presented in Section 3.5.3.

In-depth interview study: attacker-centric thinking
A qualitative data collection through 12 semi-structured interviews with senior practitioners (a corporate elite, see Section 3.5.4) at a financial services institution was undertaken as part of the research for this thesis. These semi-structured interviews were completed either face-to-face or on the phone over two cycles between August 2018 and May 2019, each lasting up to 90 minutes. Participants, working in the areas of risk, security and fraud, were asked about their background and role as well as specific questions exploring what role attacker-centric thinking played in their daily work. They were also invited to share their views on future trends they could see influencing their thinking around attackers. Thematic analysis was used to analyse the data gathered — the results from this study are reported in Chapter 8. Exact information on the data collection and analysis process including recruitment, researcher positionality specific to this study and the interview guide are described in Section 3.5.4.

3.4.3 Additional data sources

In addition to the main data sources used throughout this thesis and described in the last two sections, a small number of additional references outside of the secondary datasets described in Section 3.4.1 have been used. This has only been done for the case of the persona narrative stories (as described in Appendix A) and is also noted specifically in the methodology section for the personas (compare to Section 3.5.3, p.85). All other persona or attacker type descriptions are based on the secondary data sources as described in Section 3.4.1. The addition of these sources was deemed acceptable for the writing of the fictitious stories included in the separate Appendix A, to positively support the aspect of storytelling and create a convincing, multi-faceted narrative for each individual persona with a reference to the real world (Nielsen [29][30] on persona narratives). The nature of these sources is also in line with the larger dataset as defined in Section 3.4.1 — they consist of web links to open source materials such as newspaper articles (e.g. on money mules in The Times or The Guardian UK, see p.263) or other web resources (e.g. interview excerpts with certain attacker types or details from blogs of security researchers; see p.265 and p.261 respectively). Where these other resources have been added within the narrative, this has been clearly referenced directly within the narrative story (Appendix A).

3.5 Research procedures

The following section explains all methods and procedures used for the individual study parts of this research project as illustrated in Section 3.2.

3.5.1 Study on attacker characteristics and behaviours

NVivo 11 was used to collate and sort the documents identified during data collection based on the secondary sources defined in the last section. The software extension NCapture was used to convert all online materials into PDFs and export them into NVivo. The software was also used for coding the documents and to establish content categories as well as to create

Category/theme	Codes	Sources	Refs.
Personal characteristics	Age, alias, education, entry to criminality, gender, insider knowledge, moral code, motivation (not profit), occupation, profit (financial motivation), resources (funding and equipment), skills, social circumstances, substance abuse	181	807
Group	Size, organisation	107	224
Country of origin or residence	Africa, Australia and New Zealand, Canada, Caribbean, China, country of conviction, Eastern Europe, India, international, Middle East, South America, rest of Asia, Russia, UK, Ukraine, US, Western Europe	129	302
Targets	Geographic reach, liability, monetary damage, victims	145	305
Modus operandi	Business model, means, timeframe, risk-taking, vulnerabilities	170	392
Jurisdiction	Charges, consequences, enabler/positive factors, hindrance, investigation, rewards, sentence	160	461

Table 3.4: ***Overview of first cycle analytical codes***

and store analytical memos. Data analysis and working with the data was conducted in three distinct stages: an initial review of the source materials was attempted first to exclude all material not relevant to the overall study, followed by two phases of coding in line with the model of using various first and second cycle coding methods as described formally by Saldaña on grounded theory and its coding canon [271] p.51.

Initial review of source materials

To prepare for the data analysis, a basic review of the original dataset was undertaken to eliminate all content not suitable or directly relevant for further analysis — the significant level of reduction of this exercise is visible in the last column of Table 3.3 (where 8,725 original documents in total were reduced to 327 documents). Several factors made this review necessary: none of the original data sources as described in Section 3.4 were specific to digital banking, which means a manual review was necessary to filter out these cases (although the VERIS dataset [37] includes a marker for financial services industry). Other factors leading to exclusion were non-availability, duplication, obvious quality issues (no citation of original source, typographical and grammatical errors) or no information on cybercriminals contained.

First cycle coding and data analysis

With all materials not directly relevant to the topic of the study excluded, the coding process could begin. While Saldaña describes 25 available methods in total for first cycle coding, grounded theory generally relies on elemental methods such as in vivo, process and initial coding [271] p.53. As the source data of this study consisted of reports and fact sheets rather than participant interviews or observing their actions, this study concentrated on initial coding rather than in vivo or process coding. Initial coding (also referred to as 'open

coding' in other works on grounded theory, e.g. in Taber [269][273]; also noted in [271] p.10) is defined as "breaking down qualitative data into discrete parts, closely examining them, and comparing them for similarities and differences" (Strauss Corbin, 1998, p. 102 [274]). In summary, it enables the researcher to gain a greater understanding of patterns and issues hidden in the data while also providing a starting point for further analysis (through other coding methods or second cycle analysis) or further research (e.g. additional data gathering). But initial coding can also make use of other first cycle methods: in this study, structural coding ([271] p.84) as a method to categorise and label data to prepare for similar data segments to be analysed and compared against each other was used.

In addition, several grammatical coding methods ([271] pp.69) establishing basic information such as demographic information were used: attribute coding to label personal characteristics of the cybercriminals analysed such as age or gender, magnitude coding to assign labels of dimension (e.g. monetary damage caused by cybercriminals, high or low impact of attacks) as well as subcoding with subordinate codes (e.g. means/method of attack with the subcode 'social engineering') and simultaneous coding (where a segment has been coded against two overlapping codes). Figure 3.7 shows a coded document with all its code labels.

After the first round of coding, 51 codes around 6 themes (or category codes) were identified from the analysed documents (sources) and referenced text excerpts (items) in the dataset (refer to Table 3.4). Over 20 analytical memos and 2 rich pictures (see example in Figure 3.8) were produced, reflecting on the emerging patterns in the data, gaps and overall theme and research question of the study. Once no more new labels could be identified in the initial coding process and all documents had been analysed, split into segments and coded accordingly, the second coding cycle was started as outlined in the next section.

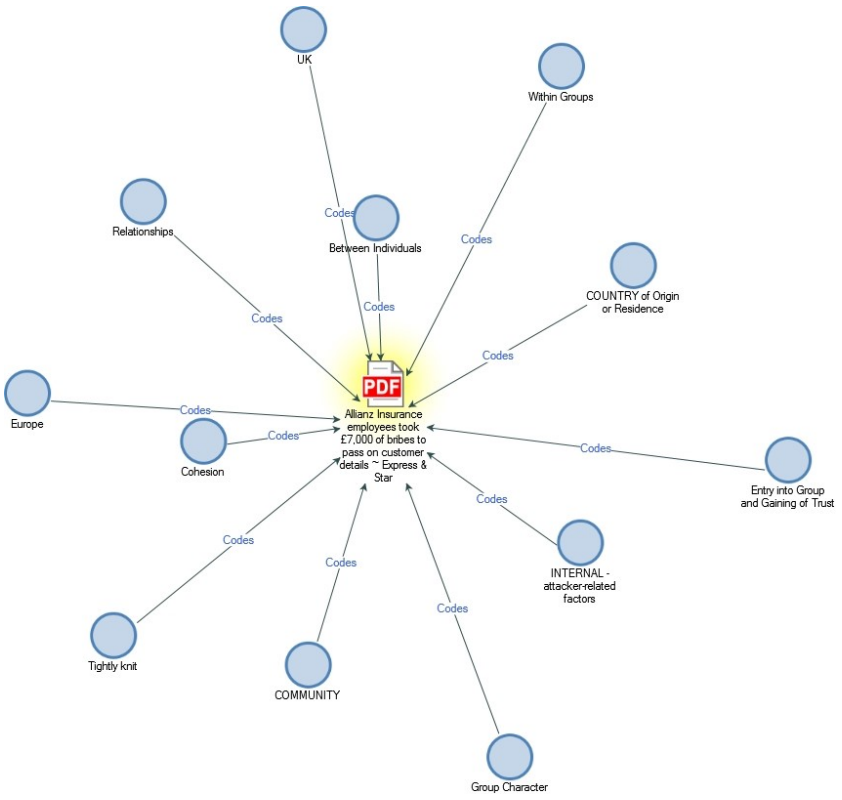


Figure 3.7: ***NVivo visualisation: example document with its code labels***

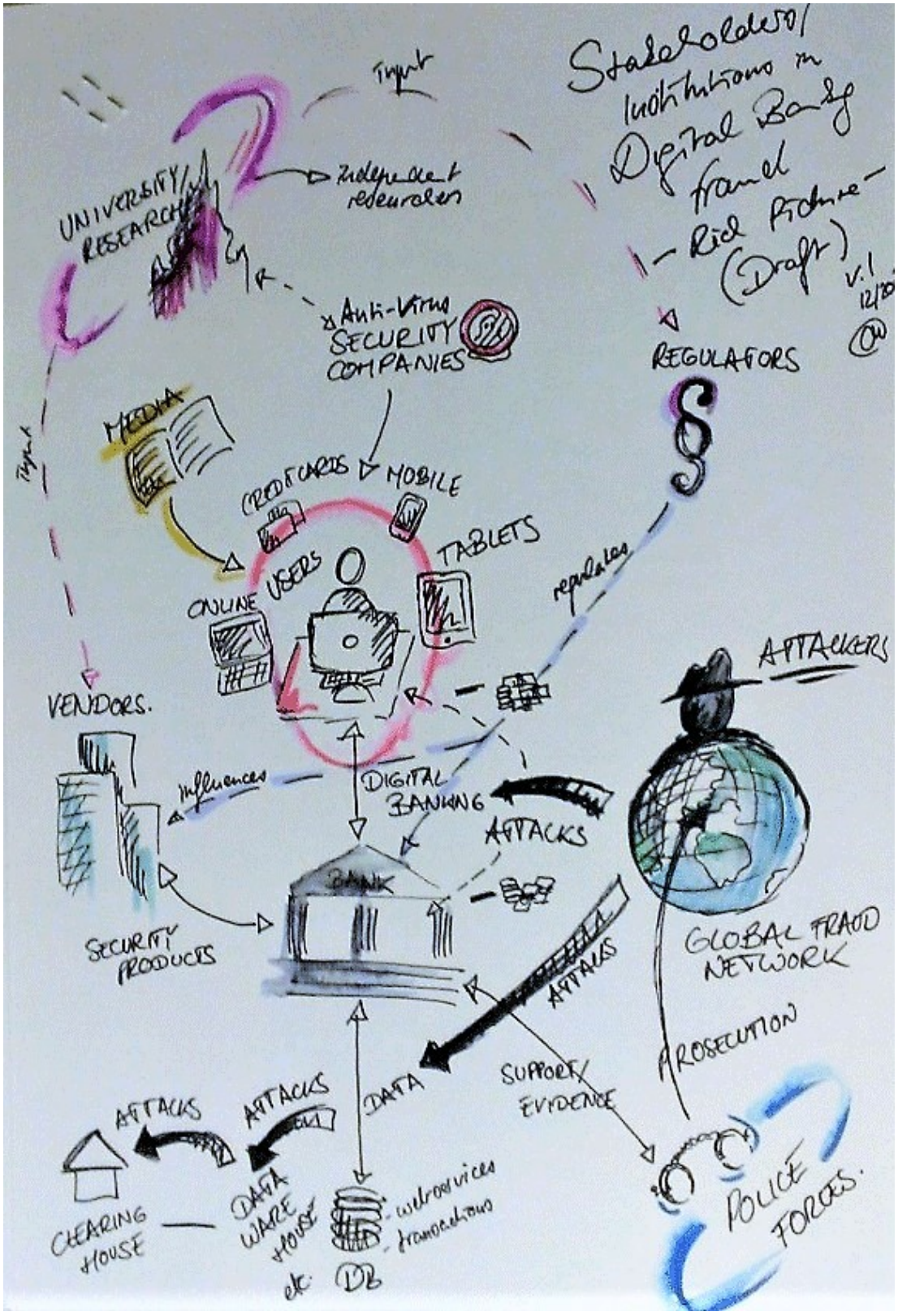


Figure 3.8: ***NVivo memo example: key stakeholders in digital banking (rich picture)***

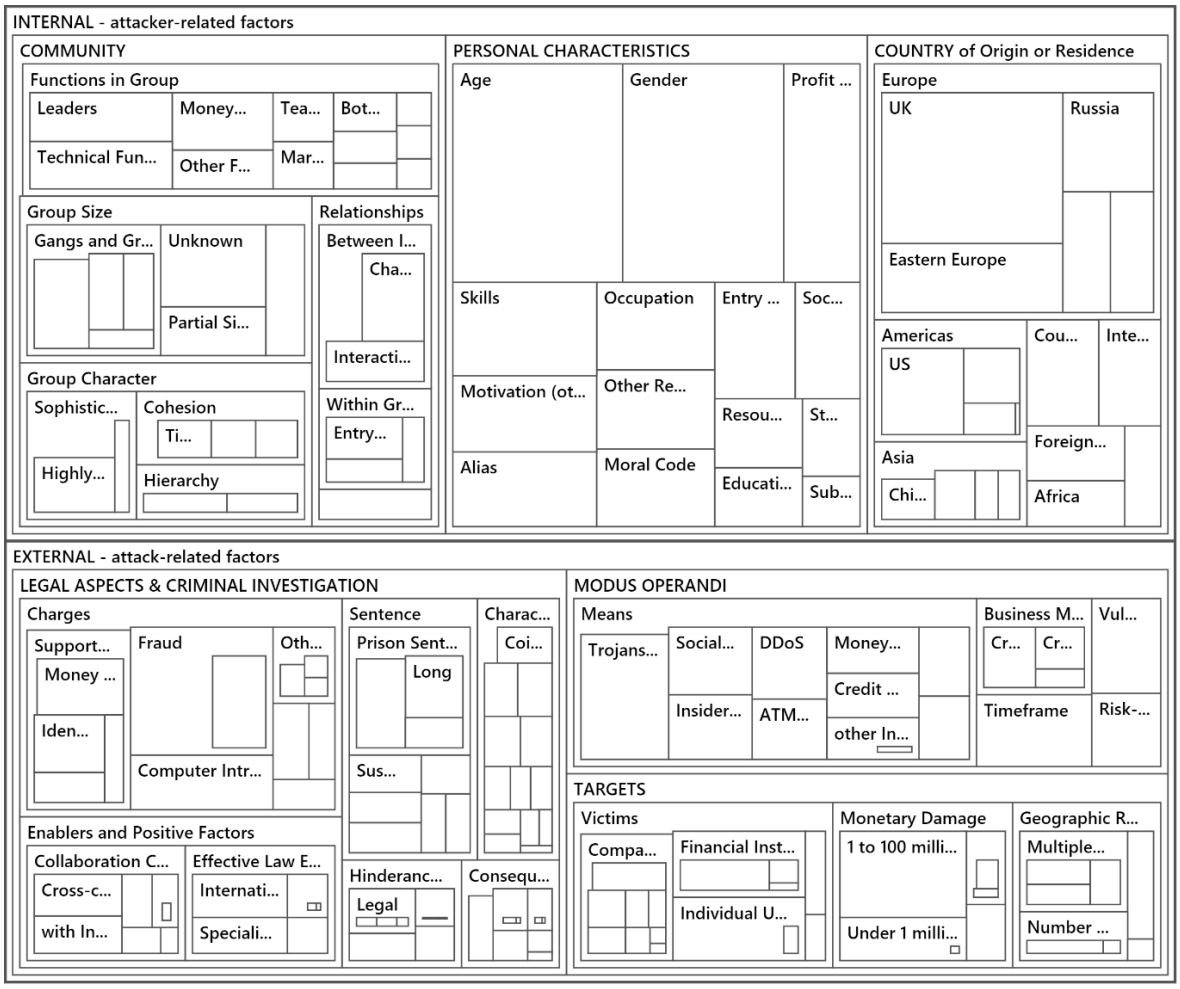


Figure 3.9: ***NVivo visualisation: schematic overview post second cycle analysis***

Second cycle coding and data analysis

While in vivo, process and initial coding methods are considered first cycle methods in the grounded theory coding canon, there are other methods for the second stage analysis when developing grounded theory: focused coding, axial coding and theoretical coding (as set out in Saldaña [271] pp.51).

From these methods, focused coding and axial coding to re-focus and review the categories from the first coding cycle were used here. These codes were then organised further into hierarchical categories around two axial main categories. Charmaz ([253] pp.60) specifies an axis as a hub category with spokes (category codes/themes) and related codes (defining properties, characteristics or attributes) and dimensions (ranges) — it is worth noting that there can be multiple axial codes developed throughout the coding process (Saldaña [271] pp.218). Furthermore, axial coding as a method is an applied concept chosen by the researcher rather than strictly emergent from data, which has sparked some debate amongst grounded theory researchers (see Charmaz [253] p.147–150; Urquhart [254] p.25/26, 191). In this research, the benefit of axial coding was seen in providing some coherence to the fragmented data and to establish a conceptual relationship between categories (in Taber [269][273]). Overall, this is in line with the informal approach proposed by Charmaz ([253] pp.148) and the examples provided by Saldaña ([271] pp.218), but in contrast to Strauss & Corbin's formal procedures in [274].

To summarise, the most significant change between first and second cycle analysis was the alignment of the initial themes or category codes to the newly created main axial codes. As shown in Table 3.6 on p.76 and Figure 3.9, two axial codes were identified as either intrinsic attacker-related factors (personal characteristics, social interactions and group structures displayed by the attackers, largely consistent overtime) or external attack-related factors (attack-related behaviour displayed, changeable over time).

However, boundaries are not always clearly defined as "there are different degrees of belonging" (Dey [290] pp.69, also in [271] p.213): categories such as e.g. country of origin or residence are part of the attacker's personal characteristics but may change over time. Other external factors (such as modus operandi) may indirectly depend on intrinsic attacker factors, for example attacker skillset. The initial collection of codes (codes column in Table 3.6) was therefore reviewed thoroughly and re-grouped where analytically meaningful — here, Figure 3.9 provides a helpful visual guide. Following grounded theory principles, the source materials were furthermore continuously reviewed against new or revised codes emerging. For the axial codes all source materials were used, while subordinate categories and codes use as many source materials as possible based on relevance. While many categories achieved a level of theoretical saturation with many attributes and characteristics accounted for, there were some coding ideas present only showing low numbers of relevant references, especially on the second and third sub code level. Where these could not be re-structured into another code, they were marked as tentative and requiring further investigation (in Chapters 4 and 5).

Proposed structure for analysis results

The results of the data analysis undertaken are presented in the next two chapters (Chapters 4 and 5). Given the large amount of data analysed as well as the high number of codes and attacker characteristics identified, a structured approach was considered useful. Therefore, results are split into two chapters, each consisting of three main sections (refer to Table 3.5). This is also in line with the structure prescribed by the axial and category codes recognised during the analytical process (in Table 3.6).

Part	**Axial codes**	**Category/themes**
Chapter 4	Personal characteristics & group structures	
Section 4.1		Personal characteristics
Section 4.2		Group structures
Section 4.3		Geography
Chapter 5	Attack-related behaviours	
Section 5.1		Targets
Section 5.2		Modus operandi
Section 5.3		Investigation & prosecution

Table 3.5: ***Structure of results presentation in Chapters 4 and 5***

Axial code	**Category/ theme**	**Codes**	**Sources**	**Refs.**
Personal characteristics and group structures			300	2487
	Personal characteristics	Age, alias, education, entry to criminality, gender, insider knowledge, moral code, motivations (not profit), occupation, remarkable characteristics, profit (financial motivation), resources (funding and equipment), skills, social circumstances and family, status/ self representation, substance abuse	252	991
	Group structures	Functions in group, group character, group size, relationship	188	838
	Geographical distribution	Africa, Australia and New Zealand, Canada, Caribbean, China, country of conviction if different, Eastern Europe, India, international/extensive travel, Middle East, rest of Asia, Russia, South America, UK, Ukraine, US, Western Europe	235	658
Attack-related behaviours of the attacker			305	2193
	Targets	Victims, monetary damage, liability, geographic reach	172	480
	Modus operandi	Business model, means, risk-taking, timeframe, vulnerabilities	251	657
	Investigation & prosecution	Sentence, charges; crime hindrances & deterrers; crime enablers & positive factors, nature of investigation, consequences of attacks	227	1056

Table 3.6: ***Overview of second cycle analytical codes***

3.5.2 Attacker typology building process

Building on the critical review of previous typologies and taxonomies, presentation of commonly mentioned attacker types and classification criteria in Section 2.3, this section outlines the methodology chosen in this thesis for creating a new typology specific to digital banking.

Past categorisation methods

As discussed in Section 2.3, early categorisation efforts have often used personal observations from a professional context (like in Gordon [133] or Ivoce [59]). They have also heavily relied, consolidated and extended on previous literature, especially works by Rogers [23][46], but also later by Meyers et al. [42]. Even newer categorisations like Hald & Pedersen [24] and Seebruck [25] have not introduced new data to the area, but used existing web resources to review the previously employed terminology. Similarly, Seebruck uses literature to explain the shift in emphasis for their typology to more ideologically and socially motivated attackers in [25]. In contrast, De Bruijne et al. [26] have introduced a systematic hybrid approach, using both a deductive approach based on a literature review and an inductive approach, e.g. through reviewing data on cyber incidents and monitoring of ongoing attacks. Several advantages can be identified for following such an approach, like the identification of new and emerging threats and attackers as well as the removal of potential bias or methodological issues from previous studies. For the proposal of this thesis, a similar approach is suggested, with an initial literature review (as conducted in Section 2.3) followed by the analysis of a dataset on digital banking related incidents (as prepared in the last section and presented in Chapters 4 and 5) to build the categorisation.

Re-coding and preparing previous data for categorisation

In order to build a data-driven typology, which can be understood as a classification and representation of groups with shared characteristics and behaviours, a reference dataset describing the items to be categorised is required. The data analysis of attacker characteristics specific to digital banking documented in Chapters 4 and 5 offers such a dataset, although this information is not yet grouped into clusters of common traits. So how is this general description of the entire, heterogeneous community of digital banking attackers then transitioned into relatively homogeneous categories, ultimately forming a typology?

Going back to the dataset and NVivo working file created (refer to Section 3.5.1), all codes describing attacker characteristics and behaviour at a relative level of detail (subordinate codes below axial codes and main categories) were reviewed for their relevance to categorisations. To help with this, previously employed categorisation criteria for taxonomies and typologies from literature (Section 2.3) were used, yielding 12 codes of interest from this original dataset (see Table 3.7). The original dataset was then coded again using NVivo, employing another round of initial coding and subcoding as methods, focussing on these 12 codes. Subcoding is a coding method that assigns a "second-order tag [...] after a primary code to detail or enrich the entry" [271] p.77. This was to ensure that all data present in the original sample and potentially relevant to the planned categorisation was captured in a structured way — in principle, this step aimed to add an additional layer of detail and depth to certain codes to support the categorisation process.

Monetary damage	Geographic reach
Business model	Means/modus operandi
Insider knowledge	Entry/paths into criminality
Profit (financial motivation)	Motivations (other than profit)
Resources (funding)	Resources (equipment)
Skills	Group-related factors

Table 3.7: ***Analytical codes including attacker characteristics and behaviour***

Re-checking and defining categorisation criteria

Rather than readily accepting categorisation from previous typologies and taxonomies, this study uses a combination of a literature review of categorisation criteria (from Table 2.2 in Section 2.3) together with a review of the 12 codes previously identified (Table 3.7) to come up with a list of own categorisation criteria (refer to Table 3.8). A similar step is included in the typology building process used by De Bruijne et al. in [26] p.16/17, who use a deductive 'first cycle analysis' to specify the "dimensions that are used in (cyber) threat actor typologies" for their research through a comprehensive literature review (further complemented by empirical interviews with security experts).

Original codes	**Proposed criteria**
Profit (financial motivation) Motivations (other than profit)	Motives
Profit (financial motivation) Business model Monetary damage	Criminal intent
Resources (funding and equipment) Skills	Resources
Means/modus operandi Business model Insider knowledge Functions in group Group character, group size	Activities
Monetary damage Geographic reach Means/modus operandi	Level of danger posed
Monetary damage Means/modus operandi	Type of risk posed
e.g. Entry/paths into criminality	Other notes

Table 3.8: ***Creating a categorisation framework: transforming codes into criteria***

Transforming the data and practical categorisation process

For the categorisation process, affinity diagrams or maps as a design thinking technique[33] were used. A comprehensive definition of affinity diagrams as a synthesis method is provided in *Universal Methods of Design* [296] p.12: "affinity diagramming is a process used to externalise and meaningfully cluster observations and insights from research" through considering data-driven insights individually and by putting them on (virtual or physical) post-it notes to then be clustered around their 'affinity' (such as similar ideas, concepts or data facets) [291]. Holtzblatt & Beyer highlight the inductive nature of affinity diagramming, based on its potential to synthesise data into clusters, and most importantly "groups are not predefined — they emerge from the data and are specific to the data" [297]. Along the same lines, Simonsen & Friberg [298] see affinity diagramming theoretically rooted in grounded theory, with both methods centred around emerging categories and ongoing comparison rather than analysing data on predefined hypotheses. Affinity diagramming exercises can be found as tools for contextual enquiry in both a scientific research context, but are very commonplace in current UX practice [294], often involving cross-disciplinary teams working on them together[34] [293]. In an academic context (specifically grounded theory generation in design research), Maher et al. [300] describe traditional material approaches (also through affinity maps) as a valuable support tool for data analysis in combination with software such as NVivo for data management facilities and larger coding exercises.

So why was this process chosen and, in contrast to all previous coding work, completed manually outside of NVivo? The researcher's background and experience (as a designer and digital experience practitioner, see also positionality statement as made in Section 3.3) contributed significantly to this: the researcher was familiar and had run similar exercises (individually or with teams) numerous times. From a practical perspective, the physical nature of this method (with the option to leave the notes highly visible on a wall for an extended amount of time) fostered emersion in the data, decision-making on grouping and overall reflection on the analytical process — this positive perception in comparison to the NVivo interface (smaller screen, less visual contact time and a fragmented overview of the data) is in line with what Maher et al. [300] label as "serendipitous encounters [...] as the researchers scan all the data looking for relationships, connections, and so on [...]". It should however be acknowledged here that such material, manual coding and analysis approaches would generally only suit working with relatively small datasets [251]. Finally, an affinity

[33] Affinity diagrams are part of the design thinking toolkit by Stanford d.school, under the label of 'saturate and group' (in [291]) or in IDEO's design kit under the header of 'bundle ideas' [292]. Design thinking (as defined and advocated by Tim Brown of IDEO in [293]) can be loosely understood as a toolkit of iterative design-type activities and enabler of taking a designer's mindset to add value in a business context, and is now widely used and taught in professional and educational settings — Kimbell [294] provides a comprehensive critique of the method's origin and contemporary usage. However, affinity diagramming dates further back in general project management and business practice and is also known as the K-J method after the anthropologist Kawakita Jiro [295].

[34] Affinity diagrams are particularly strong as a tool when used within a team — they offer a balance between enabling all participants to individually provide input, but also facilitate group exchanges through discussion. Although generally described as a team-based exercise in literature (e.g. [293] or [297]), affinity diagramming carried out by individuals or small groups are not unknown, as reported in Harboe's [299] review of real-life practices surrounding this technique. For the purpose of this study, affinity diagramming can be seen as a highly visual extension of the coding process in NVivo rather than a team exercise, although the same categorisation process could be carried out using a team scenario in principle.

mapping exercise also lends itself for replication in a corporate environment — such methods may already be known to security professionals and their teams or could be introduced and adopted easily (as described for a general business context in e.g. [297][299]).

In practice, all codes and conceptual phrases were manually transferred onto post-it notes from NVivo. Following best practice guidelines for affinity diagrams, all post-it notes were reviewed for their similarity and potential connections to others and then either placed in a new group or with an existing cluster (each representing a potential attacker type). This manual process of re-grouping, merging, removing or separating as well as naming clusters and notes contained was repeated continuously by the researcher. To aid this process, colour coding was used (see Figure 3.10 for an example of work in progress): green notes represented general codes and conceptual phrases and pink notes were categorisation labels from the data. Later in the process, yellow notes were also added for 'question marks' that needed further consideration in the categorisation: these codes potentially fitted more than one category or did not entirely fit into the criteria laid out initially (right hand column in Table 3.8). Lastly, orange notes were added to each cluster to signify the suggested high-level category names for the attacker types.

Categorisation, re-naming and re-ordering was finished when all variations were accounted for and did not present any new clues for further categorisations or changes. For this study and its underlying dataset, theoretical saturation had been reached at this point in time (defined in Charmaz [253] p.345 or Urquhart [254] p.194).

Figure 3.10: ***Example of manual clustering process in affinity diagram exercise***

From categorisation to typology: presentation of results

Using the proposed criteria list from Table 3.8, a list of description criteria was assembled to help build the attacker profiles in detail (refer to Table 3.9). With this criteria list at hand, every affinity cluster was then reviewed and where adequate details were present in the original data (and coded accordingly in the NVivo file), details were added for every criterium/aspect. The overall process required a continuous comparison and back-and-forth reviewing process between the manual cluster visualisation and the original NVivo file with its coded data fragments. As mandated by the nature of the data on digital banking attacker characteristics underlying this categorisation exercise (incomplete and often random), not all description criteria could be filled with detail from the data. Further to that, several aspects were only indicated in a single data fragment or lacked overall detail or preciseness. Where this was the case, results are presented as tentative in brackets with one asterisk* in the table view for every attacker type within the typology (see Chapter 6) — for the few occurrences where an assumption without grounding in data was made, brackets with two asterisks** are used to make this clear to the reader.

Typology validation

At this point in time, two initial validation strategies are suggested for this typology: firstly, a list of heuristics to assess the formal quality and structure of the typology close to the approach taken in De Bruijne et al. [26] (which is also relies on the work by Bailey in [142]) is used and secondly, peer review via submission at two relevant academic conferences is used to test the general acceptance of the new typology. Both validation outcomes as well as further suggested actions deriving from these are described in detail in Section 6.2.

Criteria	Description
Group	Used as a name for the attackers in this group
Subgroups	Subgroup descriptions (optional)
Labels	Describes other terms found in the sample or literature that may be used for attackers in this group
Motives	Describes the primary driver behind the criminal activity engaged in for this group
Criminal intent	Describes the level of preparedness and intent for criminal and illegal actions present in this group
Resources	Describes the resources such as funds or equipment and the skills level present in this group
Activities	Describes the main criminal activities engaged in and modus operandi used by this group
Level of danger posed	Describes the overall impact and level of destruction this group may pose to its victims
Type of risk	Describes the type of risk posed to victims
Other notes	Other obversations when studying this group

Table 3.9: ***Attacker categorisation framework: description criteria***

3.5.3 Attacker personas creation and dissemination

Building on the initial data collection and analysis of attacker characteristics as well as the typology building process, attacker personas are suggested as an extension and further visualisation of human attacker types in this thesis. Using previous insights from data and the resulting attacker typology, a detailed building exercise for attacker personas was carried out in this thesis based on a 10-step process model for building user personas borrowed from Nielsen [29][30]. To disseminate and evaluate these personas and further consider the viability and potential of attacker personas in a professional financial services setting, a survey amongst practitioners was completed following the persona build — all results are presented in Chapter 7.

Construction Notes: 10-Step Process Model

This section presents the 10 steps contained in Lene Nielsen's process model for building user personas from her works in 2007 [29] and 2013 [30]. This process model was selected based on the following requirements for an underlying framework for building the attacker personas in this work. Firstly, an approach with relatively high levels of formality and guidance to ensure potential replicability, adaptation and extension of the method was desired. Furthermore, the absence of mature methods for creating attacker personas specifically meant that a user persona creation method from user-centred design was selected and adaptations to account for attacker personas had to be made. Nielsen's framework is especially compelling as it provides a structured and sequential approach to persona building. It also incorporates learnings from many key works in persona research (e.g. Bødker & Christiansen, 1997 [301]; Cooper, 1999, 2007 [157][278]; Grudin & Pruitt, 2002 [279]; Adlin & Pruitt, 2010 [28]). A varying level of adaptation and flexibility to each step was employed to make sure the method remained relevant for attacker personas — these adapted 10 steps are now described in turn and an overview can be found in Table 3.10.

Data Collection (step 1) — initially, as much knowledge as possible about attackers applicable to the system or organisation needed to be collected. In this work, a qualitative analysis of a significant number (>300) of open-source cybercrime case studies as carried out in Chapters 4 and 5 and methodologically defined in Section 3.5.1 was used here. While quantitative data could have been used (e.g. on frequency of attack types or means), the limited availability of such data[35] in the public space influenced this decision.

- *Questions* — who are the attackers? What do they do with/to the system?
- *Methods* — quantitative/qualitative data collection
- *Deliverables* — report of findings

[35]Nielsen's method is naturally aimed at user personas. When adapting this method to attacker personas, a significant difference between users and malicious attackers to a system needs to be taken into account: user personas are often based on data directly derived from a community of users via quantitative means such as surveys or data analytics, with qualitative data collection methods such as interviews helping to shape a comprehensive persona description, this option does not usually exist for attackers. A banking institution may however have internal quantitative data available that could help build their own attacker personas.

	Process model step	Location in thesis
1	Data collection	Analysis results in Ch.4 & 5
2	Initial draft of attacker types	Attacker typology in Ch.6
3	Review of initial findings	Re-coding of original dataset underlying results in Ch.4/5 to add persona-relevant details
4	Structure of attacker persona set	Results in Section 7.2.1
5	Construction of individual attacker personas including personal details	Persona cards in Section 7.2.2
6	Definition of attacker situations and biographies	Persona cards in Section 7.2.2
7	Validation and gaining buy-in	Survey in Section 7.3
8	Dissemination of knowledge	Survey in Section 7.3
9	Creation of narrative stories	Section 7.2.3 and Appendix A
10	Continuous development/review	Section 7.4 and Ch.8

Table 3.10: ***Overview of 10-step process model as adapted from Nielsen [29][30]***

Building the initial draft (step 2) — Nielsen prescribes the creation of an initial draft[36] of attacker types at this point based on what's known on attacker types and differences between these so far from the initial data collection in step 1. Since the attacker typology presented in Chapter 6 and methodologically defined in Section 3.5.2 is closely in line with the draft description of the attacker groups as required by Nielsen's method, it was therefore used for this purpose.

- *Questions* — what are the differences between attackers?
- *Methods* — analysing the material, identifying and naming the groups
- *Deliverables* — a draft description of the attacker groups

Review of initial findings (step 3) — at this point, further data analysis or consultation with subject matter experts is recommended by Nielsen to review, verify and update the early draft of the persona set. For our attacker personas, the original data was re-coded looking specifically for data related to personas and scenarios as indicated below.

- *Questions* — data for personas: motives/inner needs/intrinsic motivations, values/moral code; data for situations: external circumstances (e.g. occupation, resources), social circumstances if known; data for scenarios: modus operandi, entry to criminality if known, level of risk and danger posed, example attacks.
- *Methods* — further data analysis/re-coding
- *Deliverables* — reflective notes/report

[36] Nielsen calls this initial draft a 'hypothesis' in her process model — here, the term 'draft' is preferred to avoid ambiguity with the usage of 'hypothesis' as a testable statement in quantitative analysis.

Structure of persona set (step 4) — after the attacker characteristics had been further fleshed out in the previous step through re-coding, this step evaluated, re-considered, consolidated or re-named the groups identified in the initial draft persona set (our attacker typology), including their importance and potential gaps as required by Nielsen [29][30]. Here, preliminary classifications such as 'primary', 'secondary' or 'additional/supplemental' may be assigned to indicate weightings in the overall set.

- *Questions* — does the initial grouping hold? Are there other groups to consider? Are all equally important?
- *Methods* — categorisation
- *Deliverables* — description of categories/persona set

Construction of individual personas (step 5) — the aim of this step was to prepare attacker persona descriptions which show enough factual detail and understanding to make the attacker personas realistic, as well as creating a level of empathy so readers can accept them as a real person rather than just a list of attacker characteristics [121].

- *Questions* — personal details (name, age, picture); background (occupation, entry into cybercrime); personality traits and social circumstances; moral code; resources (funding, equipment, skill); motives; criminal intent; activities and modus operandi; preferred targets; level of danger or potential damage and type of risk posed.
- *Methods* — categorisation
- *Deliverables* — description for each attacker persona

Definition of attacker situations (step 6) — as noted by Quesenbery in [29], the context or situation specifies the "beginning of the story, motivation for what happens, and a focus on what the persona is trying to do". For attacker personas, the motive and activities carried out including potential modus operandi strongly defined the situation, building a realistic 'biography'. Quotes from the source materials on cybercrime cases were included to illustrate the situation further.

- *Questions* — what are the needs/motives of this attacker persona? What are the situations?
- *Methods* — further data analysis for motives and situations
- *Deliverables* — short biography for each attacker persona

Validation and gaining buy-in (step 7) — Nielsen [29][30] places emphasis on the ongoing involvement of stakeholders. They should contribute and accept the personas and their situations, either through actively participating in the persona creation process or at least being asked to give their opinion. As explained in the next section, a survey type study was chosen to enable feedback on the personas and test the willingness of participants to work with attacker personas in the future.

- *Methods* — survey on persona perception
- *Deliverables* — report on findings

Disseminating knowledge (step 8) — for persona methods (and its attacker persona equivalent) to be successful, acceptance and ideally positive uptake by the project team and beyond in the organisation is needed — persona campaigns have used a multitude of methods here, ranging from e-mails and posters to events and even coffee cups (e.g. in Pruitt & Grudin [302]). In this research, the attacker persona set was shared in the context of the survey as stated above, but also via internal social media channels of a large banking institution and at two academic conferences[37].

- *Questions* — how can we share the attacker personas across the organisation?
- *Methods/deliverables* — visual representation for web (persona pack), publications [280] and [281]

Creation of narrative stories (step 9) — according to Nielsen [30], personas have no value in themselves until the moment where a persona is part of a scenario — the story about how the persona uses a future product (for user personas). In the case of attacker personas, the narrative stories describe an attack they plan to carry out, are in the process of committing or have committed, plus the surrounding circumstances. For the examples provided in Appendix A, relatively generic scenarios largely based on the source materials were created. These could however be changed for very specific cases and attacks. Quotes or statements from the original dataset[38] were used to help illustrate these scenarios. Nielsen provides very detailed guidance on writing persona narratives in [30], which can also be applied to attacker personas.

- *Questions* — in a given situation, with a given goal, how might the attacker persona go about attacking a target?
- *Methods/deliverables* — narrative scenarios for each attacker persona (Appendix A)

Continuous development (step 10) — the final step takes an outlook on the future life of the attacker persona — Nielsen [30] recommends a regular revision, approximately once a year. For attacker personas, new information or developments in the cybersecurity threat landscape, for example a sudden new wave of banking malware, may warrant the attacker personas to be re-written, re-structured, extended or eliminated. Within this research, feedback from the practitioner survey has been included and helped to revise aspects of the attacker personas presented — this is described in Section 7.3. Due to the limited longitudinal scope of this research as a PhD thesis, no further revision rounds have been completed to date.

- *Questions* — does new information alter the attacker personas?
- *Methods* — feedback from all stakeholders, new data collection
- *Deliverables* — foundation document, adaptations to persona set/personas

[37] British HCI 2019 and NordiCHI 2019

[38] In addition to the data sources used throughout this thesis and described in Section 3.4, a small number of further references in line with the original source materials were added for the persona narratives only as stated in Section 3.4.3 on additional data sources. Where these have been added, this has been made clear and they have been referenced directly within the narrative story (in Appendix A).

Survey Methodology: Perception of Attacker Personas

Surveys have been used successfully in the past to evaluate and analyse the perception of personas in the fields of UX and HCI. Billestrup et al. [303] for example questioned software developers in Denmark for their knowledge and perceived challenges around personas using an online questionnaire in 2014. Salminen et al. tested their 'persona perception scale' through a survey type pilot study, with participants evaluating three example personas each in [289] (2018). Similarly, examples of surveys involving practitioners are also found in the area of information security, for example investigating issues such as the role of an organisation's management on security culture (in Knapp et al. [304]) or user behaviour and perceptions around password systems in organisations (in Adams & Sasse [193]). As an alternative to survey research, interviews have been used to collect data concerning the usage and perception of personas in 'the wild' — in their well-cited study, Matthews et al. [163] for example interview 14 UX practitioners and designers regarding their practical, 'real-world' persona usage. Similarly, Nielsen & Hansen [305] analyse the usage of personas amongst digital professionals in Denmark with the help of interviews.

For this study, a survey was chosen as a primary collection method for the following reasons: firstly, to enable a wider distribution with more participants from various organisations and areas of work than could realistically be achieved through interviews [251] pp.155. Secondly, the aim was to provide a structured, quantitative description of common attitudes and opinions towards the attacker personas introduced in this thesis (and attacker personas in general) displayed by financial services professionals.

The survey was conducted via a web questionnaire open to invited participants[39] working in fraud, risk, security or wider IT in financial services for 8 weeks in total (months of June and July in 2019). 85 usable responses [40] were received for a set of 32 questions collecting both quantitative and qualitative data. A small pilot study with 5 respondents and a direct follow-up via feedback sessions (in person and on the phone) was run before sending out the questionnaire. A full participant information sheet (Appendix C), information on the study and the researcher was provided to all survey participants. It was made clear that participation was completely voluntary, all submitted responses were anonymous and could not be traced back to the individual. The study was completed following the relevant ethics review process of the researcher's academic institution (RHUL Ethical Approval reference Full-Review-1715-2019-05-31-11-25-PWAI216).

The sample size (N=85) was deemed sufficient to evaluate and comment on the specific set of attacker personas introduced in this thesis, with the expectation that this group would recognise the most significant issues with the personas and that this work would serve as

[39]This survey was kindly supported by the British Computer Society (BCS) Financial Services Specialist Group. The survey was sent out to approximately 1500 financial services professionals, using the distribution list of this specialist group (1200 members, via email). Additionally, members of a fraud, risk and security interest group of a large UK financial services organisation (300 members, via post on intranet page) were invited to take part.

[40]The fairly low response rate (5.6%) is potentially related to the BCS list not being security specific (it would include any IT professional who is a current BCS member, is interested in financial services and signs up to the specialist group). A usable response would be defined as a survey that was 75% completed overall.

a foundation study on this particular topic and application to financial services (as argued in Caine [306]). While the results would certainly provide insights applicable to the usage of attacker personas in organisations in general, caution would be required to not generalise these insights based on a limited sample size at this point in time[41]. Furthermore, this sample size would limit the ability for statistical analysis — in this study, a largely explorative and descriptive approach is used, which can be accommodated by the chosen sample size.

A limited bias of the participants was expected, with respondents potentially already being familiar with personas and therefore having more of an interest or stake in the research process. To mitigate this effect where possible, the invitation was worded in an inclusive manner (e.g. "There are no right or wrong answers — this survey is intended to test the personas, not you!"). Response bias ([251] p.162) was tested using wave analysis, where late responses were checked to be in line with results of earlier weeks. A further test was carried out with three non-respondents through a follow-up conversation (in person in the participating organisation), informally confirming that their responses would not significantly differ from the submitted answers. Further types of bias are related to the usage of Likert scales for recording the answers of the respondents [310]: central tendency bias (where extreme response categories are avoided), acquiescence bias (presented statements are simply agreed on) and social desirability bias (presenting themselves/their organisation more positively) — this is reflected on within the results in Section 7.4.2.

To define the questions asked in the questionnaire, the constructs introduced and tested by Salminen et al. [289] were adapted to help evaluate and test the attacker personas. These constructs are based around common criticisms found in literature for user personas — for attacker personas, certain aspects were removed as they were unlikely to be applicable (e.g. friendliness: personas are perceived as friendly by the respondent; or similarity: the respondent feels like the persona is like him or her). Every construct was filled with a number of items to make sure results could be assessed for their internal consistency, expressed through Cronbach's alpha as a coefficient of reliability [311][312] — some constructs were combined to achieve groupings of at least four items. This resulted in blocks of questions asked to the participants regarding their perception of the following constructs: clarity; completeness and consistency; credibility and empathy; relevance and applicability; usefulness and willingness. Following the guidance in Boone & Boone in [313], the questions contained in these constructs were framed as Likert-type statements with five steps (strongly agree – agree – neither agree or disagree – disagree – strongly disagree) to measure the perception participants had of the personas. Table 3.11 shows these constructs, while Appendix D lists all statement questions.

[41] To generalise the results from this study to the overall population of financial services practitioners and for attacker personas in general, a larger sample size N would be required to achieve statistical significance of the results. While the size of parent population of financial services practitioners working on fraud, risk or security topics in the UK is unknown, it would be significantly large. TheCityUK as an industry-led body representing UK-based financial and related professional services calculates the number of employees in the financial services industry in the UK as almost 2.3 million (2019 figure in [307]) — if only 5% of these employees worked with or were interested in attacker personas, the parent population would be around 115,000). If N=115,000, the ideal sample size would be 383 participants using a 95% confidence interval and a 5% margin of error. For a parent population of N=1500 (the number of people that received the survey link), the ideal number would be 306 (based on Necessary Sample Size = (Z-score)2 * StdDev*(1-StdDev) / (margin of error)2) [308][309].

Construct/theme	Items/question statements
Participant background	Job role and hierarchy level Area of work (e.g. security, fraud or risk) Familiarity with personas and attacker personas
Introduction of attacker personas	Full attacker personas set Example profile I - Bruno, the gang leader Example profile II - Kev, the money mule Example profile III - Scott, the security researcher
Clarity	Ease of reading and understanding Initial impression of complete persona set Perceived level of understanding of persona method
Completeness & Consistency	Level of information for individual personas Perceived nature of descriptions: specific not generic Match of profile pictures and descriptions
Credibility & Empathy	Familiarity with attacker types similar to personas: in the media, organisation or industry Understanding of attacker motivations Level of empathy with personas Perceived credibility of personas
Relevance & Applicability	Evaluation of learnings from persona profiles Interest in further customisation/tailoring Perceived practical value to own organisation Direct applicability of the shown persona set
Usefulness & Willingness	Perceived usefulness Tool for speaking to senior stakeholders Value for training or raising security awareness Interest in using organisation's own data Interest in persona creation exercise
Qualitative data collection	Open-ended question requesting further feedback from participants

Table 3.11: ***Overview of attacker persona evaluation survey study questionnaire***

Data analysis for this study is large composed of a descriptive analysis, reporting on data collected for each construct and related independent and dependent variables in Chapter 7 (Section 7.3). Due to the relatively small sample, further advanced or inferential analysis was not carried out at this point in time [251] p.163. SPSS was used as a supporting software tool for this study. As an initial step, all data was loaded into the software, with the Likert values recorded as ordinal numbers. Following this, Cronbach's alpha was calculated for every construct (and related questionnaire items as shown in Table 3.11) to assess internal consistency and reliability — for scores lower than .7, further enquiry and potential removal of items contained in the construct were completed to ensure reliable measurement of the construct [289][311][312]. Descriptive statistics were produced for further interpretation: means and standard deviation values for each construct (Likert scale data); mode, median (for central tendency) and frequencies (for variability) for individual questions (Likert-type data) [310][313]. The qualitative data collected through open-ended questions was examined using basic descriptive coding ([271] pp.87) due to a limited amount of usable responses (20).

3.5.4 Study on attacker-centric security in practice

To examine how digital banking professionals consider attackers in their daily practice, a qualitative data collection through 12 semi-structured interviews with senior practitioners at a case company was carried out (presented in Chapter 8). In their well-structured study on UX professionals working in an agile context, Bruun et al. [40] view such a case study approach as "appropriate for developing an understanding of a contemporary phenomenon in its real-life context" (attacker-centric thinking in a banking organisation for this study). The case company is a large European banking organisation with over 50,000 employees, covering retail, business and corporate banking with a dedicated security and risk function.

Data Collection

Managers at middle, senior and executive level in financial services institutions working in all fields of security, fraud or risk functions form a corporate elite[42]. This group can be difficult to access and recruit for in-depth interviews due to organisational gatekeeping, time constraints or lack of compelling reason to participate ("what's in it for me anyway?" in Thomas [315]). The researcher benefitted from a unique position of being affiliated with a large financial services institution, which provided an entry point for recruitment and initial access to a small group of senior practitioners who were prepared to introduce the researcher to some of their contacts in the organisation they deemed as useful for this study.

The positionality of the researcher can be described as follows: while the researcher was an employee and therefore colleague of the participants (an insider), she was also an outsider as she didn't know any of the individuals personally and had never worked with them before or even in the same area. Rather than taking a binary insider/outsider position, the researcher aimed for a collaborative, transitional perspective, incorporating both relative objectivity (outside view) and organisational and subject knowledge (inside view), guided by the works of Mullings [283] on the researcher's perspective in challenging interview settings. In addition, it was made clear throughout all stages that the position of the researcher was the one of an academic rather than a colleague at this point ('student role' in Lønsmann [284]). At the same time, the study and work with the researcher was positioned as a two-way relationship, where the researcher would feed back on the results and establish a longer-term dialogue with the participants if of interest ('consultant role' [284]).

The individuals that were initially approached held various security-related positions[43] in the organisation and had diverse backgrounds (e.g. theoretical computer science degrees or extensive professional experience in the area of fraud) as well as levels of seniority[44], which ensured an initial 'sample seed diversity' [316]. A first round of four initial interviews was held

[42] In this study, the following understanding and definition of the term elite brought forward by Welch et al. [314] in their work on working with international business elites is largely agreed on: "[...] occupies a senior or middle management position; has functional responsibility in an area which enjoys high status in accordance with corporate values; has considerable industry experience and frequently also long tenure with the company; possesses a broad network of personal relationships [...]".

[43] To help avoid identification of individuals participating in this study, general descriptions rather than their actual corporate job titles are used in the reporting.

[44] Indicative only and where known — in this specific context and for the purpose of this publication, executives would sit above senior managers in the corporate structure, with managers and senior analysts below.

	Role description	Expertise	Seniority	Round
1	Threat intelligence	Security	Manager	1
2	Threat intelligence	Security	Senior manager	1
3	Information security	Security	Senior manager	1
4	Information security	Security	Executive	1
5	Threat intelligence	Security	Manager	2
6	Operational risk	Risk	Senior manager	2
7	Operational risk	Risk	Manager	2
8	Operational risk	Risk	Senior manager	2
9	Fraud strategy	Fraud	Executive	2
10	Fraud strategy	Fraud	Executive	2
11	Fraud strategy	Fraud	Senior manager	2
12	Fraud strategy	Fraud	Manager	2

Table 3.12: ***Overview of interview study participants***

at this point (August 2018) and analysed (while two further interviews were held at the time, the interviewees choose not to participate). Given the encouraging results, a further round of recruitment was undertaken in early 2019, also looking to broaden the scope of participants in areas like fraud and risk (as recommended by first round participants). Through referrals from these initial participants, a list of potential participants (19) for a second round of interviews was identified (snowball sampling or cascading). From this list, a number of individuals (9) were subsequently excluded as they noted that attackers did not play any role in their daily work in initial informal conversations (this applied mainly to technology, digital or customer experience roles), while two individuals did not choose to participate in the study at this point. This led to eight individuals being interviewed during the first half of 2019.

In total, 12 semi-structured, qualitative interviews were conducted over two rounds between August 2018 and May 2019 (refer to Table 3.12), based on the guidelines on qualitative interviews in Patton [317] and more specifically in an HCI context from Blandford et al. [318]. The interviews lasted between 45 to 90 minutes, either face-to-face on company premises where possible, via video conferencing or on the phone. An interview guide built around three themes (refer to Table 3.13) was used by the researcher, enabling a conversational interview style without compromising on consistency. This semi-structured approach was also deemed beneficial given the relative seniority of the participants and the explorative nature of this study — the aim was to enable senior practitioners in financial services to share their own thoughts and opinions freely, however with a level of control from the researcher (avoiding a 'power shift' where the participant dominates and directs the interview [314][315]).

Adhering to company guidance to avoid audio recordings, extensive notes were taken throughout the interviews by the researcher (a process participants were very familiar with from other internal interviews, e.g. for recruiting purposes). The exact write-up of these notes was shared back with the participants for review and sign-off (via secure email channels), firstly, to aid confirming the reliability of the data collected ('member checking'[45]), but also to support

[45] Member checking is a form of participant validation — results are returned to the participants/interviewees for them to check their accuracy and the provided results matching their experiences (in Birt et al. [319]). At this point, participants/interviewees may also request to alter certain details (e.g. due to misinterpretation).

Process stage	Activities and content theme
Pre-interview: first contact point	Introduction of researcher and planned study Share general study information sheet Decision to participate/exclusion by the researcher
Pre-interview: second contact point	Option for further questions regarding study Arrange interview practicalities (e.g. time/date) Share participant information sheet Decision to participate/exclusion by the researcher
Interview: first theme — introduction	Participant's role in organisation Career pathway, education
Interview: second theme — attacker-centric thinking in daily work practices	Usage of attacker information in practice Usage of informal or formal attacker representations Examples of such representations Views on benefits and limitations of an attacker focus
Interview: third theme — future potential of attacker-centric thinking	Usage of attacker information in the future Future security trends or emerging threats in relation to an attacker focus
Feedback: first stage	Share conversation notes Re-share participant information sheet Participants to provide consent/request changes Follow-up questions/exchange materials
Feedback: second stage (optional)	Share amended conversation notes Follow-up questions/exchange materials

Table 3.13: ***Overview of interview process and structure***

the process of gaining consent in writing from all participants. This was viewed as highly important given the sensitive nature of this study, where senior members of an organisation would potentially discuss security-related aspects of their role and every day work (discussed in Moeckel [275]). This touchpoint also served as a direct feedback procedure, with about half of the participants providing additional information such as links to web resources or articles they found interesting as well as requesting minor changes to their conversation notes.

No security countermeasures or protection approaches explicit to the organisation were discussed and included in the results, thus mitigating the risk of negative implications for the organisation or individuals. It is worth noting in this context that similar information has been published by financial institutions in the past (for example in the UK by Lloyds and Barclays [320][321]). To protect the confidentiality of the participants, all data was used anonymously and identifying information was removed or anonymised. This was seen as crucial to not only avoid direct identification, but also deductive disclosure (where traits or statements of interviewees may make them identifiable [322]).

The study was completed following the relevant ethics review process of the researcher's academic institution (RHUL Ethical Approval references Full-Review-1194-2018-08-29-11-07-PWAI216 and 1624-2019-04-02-21-21-PWAI216). All participants (and potential participants) initially received a study information sheet describing the planned study and expectations if they chose to participate. Once they agreed to take part and an interview date had

been arranged, they were again provided with an updated participant information sheet (as found in Appendix E). After the interview, this communication was re-shared together with the conversation notes taken by the researcher and participants were asked to provide consent on the usage of the data collected within the thesis and related publications. All data collected in this study (conversation notes, email exchanges, participant information forms and consent confirmation) has been stored securely on a corporate/university network and additionally an encrypted/password-protected laptop/hard drive and cloud-based back-up. It is intended that data will be deleted once thesis work and all related publications are completed and/or access to these locations is terminated for the researcher. To follow data retention best practices for research data (based on EPSRC expectations and guidance [323]), anonymised data will be retained for a further 10 years[46] using an encrypted/password-protected hard drive and cloud-based back-up.

Data Analysis

A flexible and largely explorative, yet structured method of data analysis was required to not restrict the open-ended nature of this research, but without losing track of the underlying research questions posed. For this purpose, thematic analysis as a primarily inductive, iterative analysis process to identify, analyse, organise, describe and report patterns (themes) found in the data collated was chosen (following Braun & Clarke [324]). Thematic analysis is frequently used in qualitative academic HCI and commercial UX research, for example to analyse user interviews to answer theoretical questions (e.g. when investigating the role of UX professionals in agile development practices in Bruun et al. [40]) or to inform design decisions for new digital propositions (as described in their guideline on thematic analysis for user interviews by Mortensen with Blandford [325]).

Using the process description and guidance for thematic analysis in the key reference work by Braun & Clarke [324], the following six phases were completed: familiarisation of the researcher with the data, initial coding, search, review and definition/naming of themes, followed by the write-up of the final report. This study further adheres to the theoretical framework for establishing trustworthiness in research, based on a number of original criteria (credibility, transferability, dependability and confirmability as well as auditability and reflexivity) as introduced by Lincoln & Guba [326] and described by Nowell et al. in [327].

NVivo was used as a software package to support the organisation and coding of the conversation notes, review of the code structure and for the ongoing reflective memo writing. A number of different coding methods (based on the profiles provided in the coding manual by Saldaña [271]) were used for first cycle coding: attribute (codes helping with data management, e.g. to add participant characteristics), structural (codes related to research questions/discussion topics) and descriptive coding (summarising and labelling all content with a relevant topic identifier) as well as in vivo coding (for key participant quotes). After these initial coding steps, pattern (grouping together codes into an emergent theme or

[46] Although this research is not funded by this funding body, it is considered as best practice and provides extensive guidance on data retention requirements. For the exact length of time that research data should be stored, the EPSRC guidelines prescribe that "research data is securely preserved for a minimum of 10 years from the date that any researcher 'privileged access' period expires or, if others have accessed the data, from last date on which access to the data was requested by a third party" [323].

explanation) and focused coding (identifying the most frequent and significant codes) were used in a second cycle coding round. At this point, the key ideas, experiences and opinions on attacker-centric security could be observed ready for the reporting stage. Analysis and coding were initially completed for the first four interviews of the first round, followed by an academic peer review (by three senior researchers in the field of information security). The relatively low number of interviews however meant that theoretical saturation (where no new data and ideas emerge from the data collection; Charmaz [253] ch.1), had not been reached at this point in time, prompting the need for further data collection (second round of interviews). Similar themes and elements kept re-occurring approximately after a total of 10 interviews (out of 12 in total) had been completed, indicating a level of theoretical saturation.

3.6 Summary and outlook

This extensive chapter has aimed to present the research decisions and processes underlying this thesis at a conceptual, theoretical and practical level in the most transparent and comprehensive way possible. Firstly, the larger conceptual framework including the usage of grounded theory for the basic data analysis, but also the main theoretical aspects shaping the typology build and the attacker persona creation (and how they relate to previous works and theories) have been outlined in this chapter. As this work consists of several interrelated parts building on and referencing each other, care was also taken to explain the overall sequencing and structure to guide the reader through this thesis. Similarly, the data sources — both of primary and secondary nature — informing this research have been comprehensively laid out in this chapter.

In a more practical manner, the second part of this chapter has shown the detailed procedures behind the different study parts, from the basic data analysis on attacker characteristics and behaviour that underpins almost the entirety of this thesis, the categorisation (typology) and visualisation tools (personas) and finally the explorative collaboration with individuals in the financial services industry to understand their perspective on attackers and attacker-centric security (in-depth interviews).

The results from these research processes are then presented as follows in the remainder of this work. The results from the data analysis on digital banking attackers and their characteristics and behaviours are shown in Chapter 4 and 5, where Chapter 4 shows the findings relating to personal characteristics and group structures. In contrast, Chapter 5 focusses on attack-related factors and attacker behaviour. The results presented in these analysis chapters (forming Part III of this thesis after the introduction and research design as Part I and II) then lead up to the fourth part of this thesis (Part IV: Meta-Analysis) consisting of three chapters (Chapters 6, 7 and 8). The findings from Part III are used to help build the attacker typology specific to digital banking in Chapter 6 — this work is then extended to inform the attacker personas in Chapter 7. Chapter 8 then concludes the meta-analysis by opening up the discussion on attacker-centric security with the interview study with financial services elites. To wrap up this thesis, Part V then includes concluding remarks and suggested future work in the area.

Part II

Analysis

The people involved are not necessarily sophisticated or even high tech, criminal masterminds. They are everyday people with a motivation and an opportunity. Almost anyone can do it.

— F. Varese and J. Lusthaus,
Oxford University,
2017 [239]

4

Personal Characteristics and Group Structures

This chapter presents analysis results regarding the personal characteristics, social interactions and group structures as well as geographic distribution shown by digital banking attackers in our sample. Where deemed useful and possible, references to related literature are made. A summary of key points and reflection on our findings is provided at the end of this chapter.

This chapter and its subsections are defined by the code structure which has emerged during the data analysis stage (compare to Figure 4.1). The first section presents the list of personal characteristics attributed to digital banking attackers in our sample, followed by a section on community factors. Observations on their geographical distribution are also made. The presentation of data analysis results is continued in Chapter 5, which reports on attack-related factors (in contrast to attacker-related factors as described in this chapter) as observed in the sample.

To emphasise the grounded nature of this research and connection to the original dataset analysed, direct quotes from (or at least references to) the over 300 documents within the source dataset as specified in Section 6.4.1 are used where possible. A full list of the analysed materials is provided in Appendix B of this work — where specific documents have been referenced, they are denoted as e.g. [B123] outside of the standard bibliography list. Using this format, references in this chapter (and subsequently Chapter 5) will either refer to the document content in general, e.g. on p.101: "[...] criminals may involve their spouses (e.g. in [B19][B46][B166][B179]) [...]" or include specific quotes like on p.105: "he spent it on

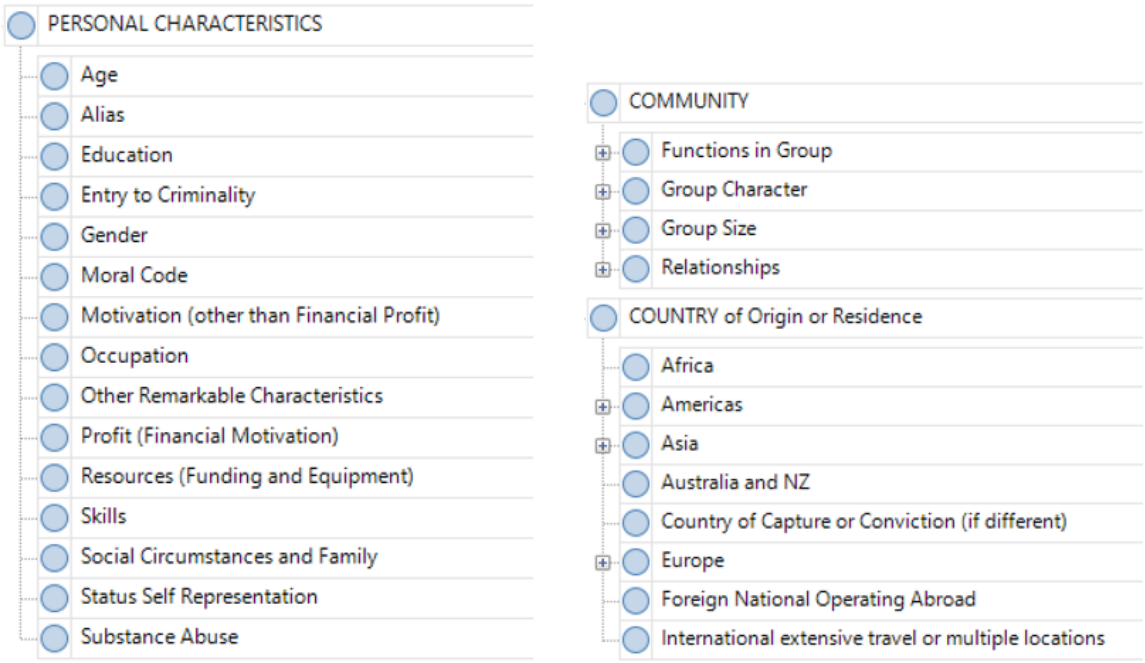


Figure 4.1: ***Emerging code structure from data analysis (attacker-related factors)***

travelling and a luxurious life, like flying first class and staying in luxury places [B9]". Where references to external materials outside of the analysed datasets (e.g. to previous related literature) are made in Chapters 4 and 5, these are naturally included in the standard bibliography at the end of this thesis.

4.1 Personal characteristics

As indicated in the introduction, this section reports on analysis findings regarding personal characteristics of digital banking attackers. Codes related to these characteristics, as they emerged from the data during analysis (see Table 4.1 and also Figure 4.1 previously), are used to structure this section into 11 subsections. Initially, five general descriptors of digital banking attackers as found in the sample data are described (age and gender, typical education and occupation as well as personal circumstances). This is then followed by an assessment of their moral code and paths into criminality as observed in the sample. Next, the motivations of such attackers, their resources and skills are reported on. Where codes only show a limited number of sources and references attached to them, findings are classed as (currently) tentative — to address this issue, references to existing literature are made where applicable — e.g. to the work of Chiesa et al. in the context of their *Hackers Profiling Project* [93]. While each of these 11 subsections are self-contained, a brief overall reflection is provided in Section 4.4 at the end of this chapter.

4.1.1 Age

For the 314 occurrences relating to age in the sample, the average age (arithmetic mean) is 31.06, with a median value of 29 and a mode value of 27. The standard deviation in the

Codes (first level)	Sources	References
All in category code	246	968
Age	143	205
Gender	140	202
Education	16	18
Occupation	59	68
Personal circumstances	70	113
Entry into criminality	31	42
Moral code	40	60
Profit: financial motivation	56	74
Motivation: other than profit	52	83
Resources: funding and equipment	21	23
Skills	45	54

Table 4.1: ***Coding overview for personal characteristics category code***

sample is 9.54 and the maximum variation in the dataset is 53 (age of youngest individual: 15 years old; age of oldest individual: 68 years old).

When analysing the age of suspects in relation to certain crime types, the sample shows some tentative patterns — while this is certainly interesting, these results are only of limited explanatory power as the sample is fairly small and needs to be treated as such.

- For social engineering cases, the average age of suspects is 31.71 years (21 references in total identified in sample).
- For insider crime cases, 31.31 years (29 references)
- For hacking offences using malware, trojans or viruses, 28.5 years (24 references)
- For cases involving DDoS attacks, 25.58 years (19 references)
- For phishing cases, 29.5 years (25 references)
- For ATM fraud, 32.66 years (35 references)
- For money mule cases, the picture is less precise, but the average age of a money mule in the sample seems to be between 20 to 30 years old, although a wide age spread (22–55 years) exists for such support functions. Mule operators and mules involved in more complex operations are likely to be older in the sample.
- For ages in groups or gangs, the sample indicates that smaller and tight knit groups seem to be more homogeneous in age, while larger, loose groups with a more corporate-like organisation have a larger spread.

As there seems to be no other datasets or studies specific to characteristics of digital banking attackers available, these results can only be compared to general literature and public information at this point. These external figures show some variance for the average attacker age: the UK National Crime Agency (NCA) for example stated the average age for UK cybercrime suspects in 2015 was a low as 17 years old [328][329]. The *Hackers Profiling Project* [93] suggests that there is no common age for hackers: although most of them would be adolescents,

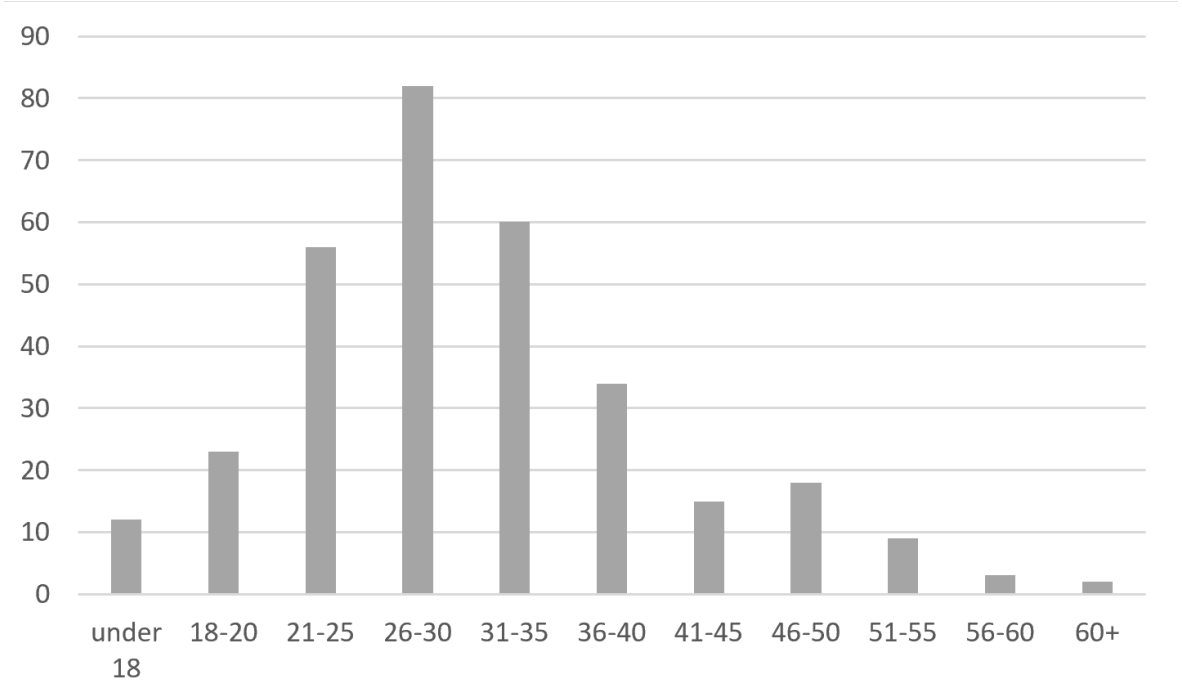


Figure 4.2: ***Overview of attacker age distribution***

their average age will have increased over the last decade as people are still hacking, bringing their age closer 30 to 35 years. In contrast, Goodman [330] suggests the average age to be as high as 35 years and the sample used in Marcum et al. [331] on convicted cybercriminals in the US also shows an average age of 35.9 (including a relatively high standard deviation of 10.41). An interesting statistic is presented by HackerOne [332] in their 2020 report on their community of white-hat bug bounty hackers, where 83% of hackers are under 35 years old (18–24: 42%; 25–34: 41%) — although a mininal increase in older individuals (35–49 age group) is noted (up to 12% from 9% in the previous year).

While the relatively young age structure (85% under 40 and nearly one third under 25 years old) in our sample is in line with other statistics, the wide spread of ages (compare to Figure 4.2) present in the sample is interesting. This could be due to the varied nature of cybercrimes and criminals present in the sample, ranging from hacktivists, botnet creators and virus writers, criminal gang members with various roles to money mules and other supporting figures who are not directly engaging in the technical 'hacking' process. For the case of digital banking, the age range of cybercriminals involved seems to be moderately young with the average attacker aged around 32 years old and the majority aged between 21 to 35, although there are outliers with teenage hackers aged under 21 and significantly older criminals (visible in the general distribution and tail on the right side of Figure 4.2).

4.1.2 Gender

Cybercriminals in our sample are predominantly male, with only 31 females present (out of 314 individuals mentioned) in the overall sample (9.87%). This is in line with other research, for example in Ziegler & Fötinger, where their reviewed sample contains under 6% female attackers (35 out of 599 in [140]), or similar figures provided by the UK NCA [328] or

HackerOne [332] (10% of their hacker community identified as female or non-binary). The age distribution for female individuals is only slightly higher than for the male group, with the average age and arithmetic mean at 31.86 (31.06 for males in the sample). The youngest female individual in the sample is aged 16 and the oldest 55 (data range 39 years).

Regarding crimes committed by female cybercriminals, the small sample of only 31 individuals does not allow for a statistically valid assessment. The cases recorded however indicate a high amount of fraud and money laundering for females (13 and 11 case examples respectively, e.g. in [B50][B149][B222]). There are also several cases where women play a supporting role (11 references), often for their partner who is committing a cybercrime offence, e.g. in [B46] or [B153].

4.1.3 Education

The sample provides an interesting and varied picture with regard to the education level of cybercriminals engaged in attacks against digital banking. Attackers who have gained formal qualifications such as computer science degrees or MBA degrees [B116] (or are currently working towards a formal degree, e.g. in [B155]) are mentioned in the sample, just as attackers with no formal qualifications (although they may possess self-taught hacking skills and 'advanced computer knowledge', e.g. in [B54]). One reference also describes the high levels of intelligence found in these individuals: "the hacker had never studied computer science but is described by prosecutors as extremely smart" [B18].

Several references highlight that these high levels of education and intelligence paired with unemployment and a lack of opportunities for young people in environments of weak law enforcement and higher prevalence of corruption in a country may lead to young people getting involved in cybercrime: "Russia I think has the highest number of science graduates, second highest number of engineering graduates in the world, so a lot of technical, high-level education being provided in those countries" [B81], similar in [B104].

Somewhat surprisingly, educated individuals can also be found on 'the other side' of cybercrime, in lower level but high-risk roles, for example as money mules: [B94] i.e. describes cybercrime as a trap for the "gullible educated youth". The latest NCA report on pathways into cybercrime [328] also discusses this 'easy route' of young individuals into cybercrime, regardless of their background (no socio-demographic bias). In their report, education also plays a secondary (reverse) role not indicated in the sample: education, together with positive opportunities and role models for young people, may provide a way out of the criminal environment of cybercrime.

Overall, it needs to be recognised that not only highly educated and skilled individuals play a role in digital banking cybercrime — the breadth of roles and methods used in digital banking cybercrime offer opportunities for many personalities and skillsets. At the top end of the spectrum however, highly intelligent and skilled individuals, whether through formal or informal education methods, can be found.

4.1.4 Occupation

Similarly to their education, digital banking attackers can be found in many occupations and professions — this is not surprising given that because there are so many facets to cybercrime against financial services, there are many paths into cybercrime and roles to fulfil. Those in the sample include students (e.g. in [B41][B101][B186]), the unemployed [B138][B140], IT specialists (e.g. in [B185][B288]), individuals in professional roles such as accountants (e.g. in [B189][B205]) or financial services workers (e.g. in [B165][B222][B290]) as well as professional criminals, but also gym instructors [B209] and professional football players [B132]. Naturally, individuals working in the area of information technology, computer science and information security as well as banking professionals make up the largest proportion of occupations found in the sample (57 out of 84 individual occupations specifically mentioned in the sample — as the 59 documents referenced often included more than one individual or were not precise in their attribution, the number of occurrences are recorded as accurately as possible here).

For further clarity, the encountered occupations can be split into four groups:

1. *Occupations not related to either information technology or banking* — individuals in education or higher education (secondary school or university/college), individuals described as unemployed, individuals described as asylum seekers or refugees (e.g. in [B159]) or individuals in unskilled/support roles. Digital banking attackers in higher skilled or managerial roles outside of information technology or banking were not identified in the sample (14 references).

2. *Occupations related to information technology* — general information technology roles, e.g. computer specialist for a payments service provider, employee of an internet service provider, computer/network engineer and software programmer, internet entrepreneur, web designer or developer, IT expert in a medium-sized company or specific information security roles, e.g. director and owner of a private information security company, computer hacker (white hat), co-founder, manager or employee at private security computer companies, information security specialist based at universities and technology companies (20 references).

3. *Occupations related to financial services* — financial services roles, e.g. customer support executives in call centre, bank workers (unspecified), various roles at third-party suppliers (e.g. payment services or accountancy firms) or IT roles in banks. An overlap between IT and financial service occupations may be observed (37 references).

4. *Professional criminals* — the last group of occupations found in the sample can be defined as professional criminals: these individuals have no other occupation and are alternatively named 'fraudsters' based on them specialising in digital banking fraud, 'hackers' or 'guns for hire' (13 references).

4.1.5 Personal circumstances

There are several references to life circumstances and personal relationships of digital banking attackers in the sample. Given the large variation of attackers encountered in the sample,

a range of contrasting aspects are to be included here. However, it can also be expected that personal circumstances of some attacker types will not be touched on in detail as no references are present in the sample (for example for members of large criminal gangs who have not been reported on widely).

Attackers do not necessarily differ significantly from other populations of individuals and may lead a relatively normal life, living in quiet, leafy suburbs with their children [B121] or operating from the bedroom of their parents' house [B11][B150]. They may be well integrated in society and even claim tax credits, housing benefits, income support or jobseekers' allowance, as mentioned in [B173], "totally at odds with somebody receiving tens or hundreds of thousands of pounds a year into their bank account".

Similarly, many references hint at existing relationships and marriages (e.g. in [B19][B39] [B168][B185]), although the quality of these relationships remains unconfirmed in the sample. And even once attackers have been prosecuted as criminals, a positive family environment can help rehabilitation, i.e. in [B146] on a young 'gun for hire' who was engaged in large-scale DDoS attacks and credit card thefts: "his family have since played a key role in supporting his recovery to the point where he is now completing his A-levels and hoping to go to university". These findings are generally in line with the survey results from Chiesa et al. [93], where most respondents do not fit the stereotype of the antisocial 'loner' or 'geek' hacker (p.96). This is supported by Thackray in her study on group processes and social identities within online hacking communities, where interview participants positively mention social aspects and interaction with other peers [94] p.100.

In contrast, the sample also includes several references for vulnerable individuals facing difficult personal circumstances that may drive them into cybercrime, i.e. in [B233]: "this is a serious level of offending, but it's occasioned by an extremely damaged person". These difficult situations range from stress at work and marriage problems [B165] to severe cases of domestic abuse: "appalling degree of abuse throughout the entirety of her life" in [B222]. Mental health issues and personality disorders are also described to affect the attackers in several cases in the sample [B39][B48][B128]. Personal debt or financial difficulties of family members are also likely to put pressure on individuals, potentially making them susceptible to engage in criminal actions when the opportunity arises, i.e. in [B159], where an individual was "promised a cut of what was stolen from Halifax Bank customers, money that he planned to send to his family in Lithuania who had financial difficulties", with similar examples also in [B138][B164]. Living as a refugee or asylum seeker, as mentioned in a few source documents, is another circumstance that could place a strain on individuals and lead them into cybercrime [B130][B159]. Substance abuse, either of illegal drugs [B15][B38][B201] or prescription medicines [B285], may also play a role for vulnerable individuals becoming involved in cybercrime.

Lastly, the social component of engagement in cybercrime needs to be considered. While being part of a group of attackers offers positives in terms of social cohesion and identity (as discussed next in Section 4.3), it may be the real-life social contacts and influence of others that brings individuals into cybercrime in the first place. This is evidenced in the sample by a number of cases — criminals may involve their spouses (e.g. in [B19][B46][B168][B185]) or other relatives (e.g. brothers or sisters in [B10][B180]) to support their activities. Wider

social relations such as friends, acquaintances or colleagues (e.g. in [B171]) may also be recruited as well as online contacts (for example through forums or social media, e.g. in [B54]).

4.1.6 Entry to criminality

While many cybercriminals who decide to attack digital banking services are motivated by profit (refer to Section 4.1.8), there are other motivators, e.g. curiosity or thrill-seeking (Section 4.1.9). How do individuals then start their criminal cybercrime career and enter cybercrime?

In our sample, the most common starting point is the internet itself. Online forums, social media and other channels such as the darknet serve as an information source, collaboration space and meeting point for cybercriminals starting out: "the duo met through an online 'hackers' chat forum, and started their criminal activities [...] within a short space of time they escalated their criminal enterprise to sell compromised credit card data [...]" [B54] or "they recovered chat logs from cybercrime forums, showing (he) was conspiring with crooks from Russia, Lithuania and the UK to hack computers and defraud associated bank accounts" [B221]. They are also the place for carrying out 'business' with other cybercriminals: "while he was looking for credit card cloning related websites, J came in contact with Nigerian O at an online chat community. J purchased data of international credit and debit cards [...], a skimmer and two card readers" [B116]. Like in these examples, the advertising of cybercrime supplies is often also happening through internet channels, e.g. in [B93].

Many individuals, showing various levels of readiness to engage in criminality, are actively recruited into cybercrime. This can happen in a rather informal way via friends or through their social circles: "to conceal the large sums of cash flowing into his bank account, Moore recruited two friends" [B207]. Most recruitment activities however are of a professional nature as made evident in the statements by T. Oerting, the former head of the European Cybercrime Centre (EC3), who talks about the lengths that organised crime will go to recruit and retain young technological talent and that criminal gangs were actively recruiting young programmers from universities, talent-spotting online to identify creative programmers [B99]. Non-technical support functions may also be attracted through professional recruitment campaigns and even genuine channels: "the mule in this case had been hired through a work-at-home job offer after posting her resume to a job search site" [B301].

As indicated in the last section, vulnerable individuals may find themselves drawn into cybercrime in situations such as economic hardship or large indebtedness, for example in the case of money mules, e.g. in [B101][B302] or even to pay back outstanding taxes [B288] or other gang members [B294]. Young people "at risk of entering into serious forms of cybercrime" [B199] are therefore of particular interest to law and governmental organisations. Here, the general expectation would be that an early interception and rehabilitation will prevent them going further down the criminal path and instead start a career in the field of computer science [B199].

4.1.7 Moral code

There are a number of references relating to the attackers' moral code — a set of rules that governs what is right or wrong for the individual. Attackers targeting digital banking and its users (and therefore turning other humans into victims[47]), face a number of ethical decisions, although they may not always be aware of the involved morality. In many cases however, the attackers willingly accept the impact of their actions on other individuals or corporations in return for financial gain.

Many attackers in the sample abuse a position of trust to commit their crimes — this can be trust placed on them by an employer, customers or other individuals. Bank employees are trusted to have access to sensitive personal data, which can make the impact of abusing their position rather significant, as evidenced in this report on a call centre worker extracting customer information and passing it on to external accomplices: "you began abusing that trust only four days after commencing work; for a period of ten months after [...] the bank and customers were defrauded by not far short of a quarter of a million pounds" [B222], similar in [B156][B162][B165][B215].

External attackers may also use the naturally high level of trust customers place in their bank and its employees to their advantage, for example when sending phishing emails in the name of a banking institution [B139]: "(attackers) profited enormously by taking advantage of the trust that many of us would place in an internet service that appeared genuine". In the case of social engineering and other fraud schemes that require direct contact between the attacker and the victim, the attacker will also try to establish an initial level of trust before abusing this position [B130][B193].

By abusing the trust placed in them, attackers accept the wide-ranging and often devastating impact the attacks may have on the victims. They accept causing large financial losses: victims may be pushed into debt, lose their life savings [B148][B159][B185][B191][B193], their house [B191] or business [B155][B176]. In addition, personal fraud losses may also have a negative impact on an individual's relationships: "this has impacted upon my relationships with my friends and family" [B191], similar in [B193], or their own health and wellbeing: "I can't sleep at night and my husband and I have been fighting" [B191], also in [B159]. Attackers will not only accept causing harm to private individuals, they will also often be prepared to harm their employer, showing minimal levels of loyalty or respect to them and their customers [B6][B94][B120][B156][B162][B165][B215][B222] — also in [B210]: "(he) took the decision that his employer was going to be the one to foot the bill for his payday loans and drug debts".

[47]The term 'victim' (or potential victim) as used within this section and subsequently in this thesis denotes all individuals harmed (or potentially/at risk of being harmed) physically, emotionally or financially (based on the definition provided in the Code of Practice for Victims of Crime UK [219]) by attackers and their actions such as defrauding, internet scams or other cybercrimes (ActionFraud UK [333]) specifically in a digital banking context. This definition is also in line with industry examples, e.g. by the Royal Bank of Scotland in [334]. It is worth noting that further aspects of victimisation, the role of the victim in crime and interactions between victims and offenders as examined in the research field of victimology [335], are not considered in detail within this work and its dedicated focus on attackers/offenders. However, related aspects as emergent from the data analysed such as type of attack targets and victims affected as well as hurdles to cybercrime investigations and effective responses are included in Chapter 5.

Not only do they accept all these implications for the victims, they often target the most vulnerable in their attacks. This may mean individuals who are in debt [B214] or the elderly [B130][B191][B285][B311] — in [B191], fraudsters are reported to have maintained 'suckers lists' with details of individuals susceptible to their scams. Small businesses without sophisticated security protection may also be of particular interest to certain attackers [B162]. This principle also applies when recruiting money mules: "criminals frequently target vulnerable victims or those keen to make some quick money" [B143]. Attackers may not only target the most vulnerable, they may also take advantage of those close to them, ranging from their neighbours [B140], family [B16] to their spouses [B180] in the sample. The moral code of attackers (e.g. ex-employees or company insiders) may also stretch to the conspiration with professional criminals (e.g. in [B130][B162][B180][B215][B222]).

Given the level of harm at a financial, but also at a personal level for the victims, do they show remorse for their actions? In the limited cases included in the sample, this ranges from attackers showing no remorse at all: "he continued to offend following his arrest with an arrogance that is unbelievable" [B191]; or "but you have shown not one drop of remorse for the fraud with which you were involved" [B159] to cases of attackers being very remorseful (e.g. in [B164] or [B307]) and showing "complete and genuine remorse" with virtually no risk of further harm or re-offending [B146].

Lastly, there are several other aspects to consider in the context of morality and the values attackers adhere to — as these have only been mentioned in few data sources, they need to be considered as tentative indicators requiring further data input and analysis. Attackers may feel strongly about other attackers working together with law enforcement officers — a commonly shared moral code prohibits handing others in [B134]. There may also be moral codes or unwritten rules specific for some groups of attackers, e.g. not to commit crimes against their own country [B114] or to specifically commit crimes against certain countries [B256][B320]. Certain attackers or groups of them may also have their own, non-conventional idea of morality and potentially their own internal sense of justice: "I do whatever I feel is right at the time" (hacker Mike 'hann' Major Jr. after disrupting the international hacking collective LulzSec, in [B55]), actions against financial services providers by hacking group Anonymous [B10][B123][B287][B310] or exposing vulnerabilities or data publicly resulting in considerate risk, reputation loss or privacy breach (e.g. in [B29][B320]).

4.1.8 Attacker motivations: profit

A strong driver behind digital banking attacks and for its attackers is monetary profit, as supported by a significant number of direct references in the dataset (74). Within this sample, attackers motivated by monetary gain seem to range from attackers looking to 'make a living' as cybercriminals (like they would with any other ordinary occupation) to attackers earning very significant sums (most likely beyond their earning potential through following a lawful career path).

For the first case, cybercrime seems like a logical alternative in areas of the world where gainful employment is hard to come by, e.g. for 'cashers' supporting large-scale cybercrime by withdrawing funds from ATMs and receiving a share in return (as much as 30 to 50

percent in [B326]). But highly skilled individuals may also be drawn into cybercrime against banks for the same reason: "people think: I've got no money, a strong education and law enforcement's weak. Why not earn a bit on the side?", says a 21-year-old hacker in [B104]. And not all criminals will spend their profits extravagantly, but use them for their rather mundane hobbies (like computer equipment or their motorbike, in [B156]). Several cases in the sample also report the cybercriminals sharing some of their illegal wealth and supporting their relatives by gifting them some of their income, e.g. in [B164] and [B54].

As a darker side to individuals relying on cybercrime for income, desperation, debt and drugs may play a role as a motivator. Money mules especially may find themselves in a position where their situation seems so hopeless that engaging in cybercrime seems the only way out, e.g. in [B209]. Pressures from outstanding debts may also accelerate this downward spiral into crime: "(he) stated he used (the) majority of the cash to settle pay-day loans and drugs debts before spending the remainder on a car, holidays and other luxuries" [B210].

These cases are in strong contrast to cybercriminals using their profits to fund a luxurious lifestyle. As the profits through cybercrime often seem unlimited to the individual, they will spend money on luxury products ranging from cars, luxury shopping sprees including jewellery and watches or holidays and travelling. There are many examples in the sample of cybercriminals using their profits in this manner: "with his gains he was able to purchase among others a top of the range BMW with a personalised registration plate valued alone at more than £10,000" [B207]; "(he) partied with pop stars while splashing out on Rolex watches, jewellery and trips to Dubai, London's Southwark crown court heard" [B191]; "he spent it on travelling and a luxurious life, like flying first class and staying in luxury places" [B9] or "according to British prosecutors, the two lived a 'jet set' lifestyle and spent money on holidays, cars and property" [B168]. The sample however also records cybercriminals investing their money in a more sensible and sustainable manner — to buy (luxury) properties in their home countries or abroad [B6][B85][B107][124][B168].

4.1.9 Attacker motivations: non-profit

In contrast to profit-driven attackers, a range of non-profit motivations can be found in the sample — however, the overall number of references is relatively small, limiting the confidence levels in these findings. In this sample, the two main non-profit motivated attack types against banks and financial institutions and their services fall into the areas of cyber activism ('hacktivism') as well as nation-state sponsored attacks.

Prominent cases of hacktivism include DDoS attacks on financial institutions (PayPal and Mastercard) which had stopped supplying banking services to WikiLeaks (a platform for news leaks, secret and classified information from anonymous sources), e.g. in [B218] or [B10]. But financial institutions may also be targeted by lesser-known attacker groups, where attribution is not always entirely clear — e.g. in the example of the 2012 DDoS attacks against numerous US banks by activists with an assumed religiously motivated agenda [B108] or other less publicised DDoS attacks, e.g. in [B259][B261] or against Russian banks in [B298]. Financial services institutions may also become victim of website defacements, e.g. in retaliation for their support of certain causes or political parties [B276][B280][B282][B286][B297] or to

attract awareness publicity for the attackers' own cause, e.g. "the Syrian hacktivists who defaced government websites from all over the world in an effort to raise awareness of the situation in Syria" [B300].

The exact reasons for why financial services institutions are being attacked at a certain point in time is not always clear — while the support of a political agenda, retaliation [B69], moral reasons (including animal rights in [B273]) or religious beliefs may play a role as mentioned in the examples above, these altruistic motivations may also blur with financial motivations. The case of attacker collective Anti-Sec is considered to be an example of such behaviour: "many who have lined up beneath the banner of Anti-Sec were disguising what would otherwise be called petty vandalism" (R. Ferguson, director of Trend Micro's European security research in [B123]). Attacker group Rex Mundi similarly acknowledged money as a motivator by publishing the following on social media platform Twitter: "we <3 hacktivists like @AnonymousPress. However, we're in it for the money, which is also pretty awesome" [B320]. Smaller groups (e.g. Tusobola Net in Kampala, Uganda [B121]) which initially identify as hacktivists, but ultimately engage in cybercrime for personal financial gain can also be found in the sample.

Cyber activism is not only close to financially motivated attacks, it may also be backed by nation states to be used for a government's political agenda, e.g. suspected in [B108]. There are various indications of nation state sponsored attacks affecting banks and financial institutions in our sample. However, there are few definite details for these incidents mentioned about the parties involved. This is most likely due to the secretive nature of nation state sponsored attacks and the effort that goes into disguising their involvement to avoid open political conflicts with other nation states. Examples in the sample include suspected attacks against the US financial sector [B242] from a group based in Iran and potentially backed by the Iranian government as well as cases of Chinese attackers against US targets, in [B6]: "US government officials have been reluctant to tie the attacks directly back to the Chinese government, but analysts and officials quietly say they have tracked enough intrusions to specific locations to be confident they are linked to Beijing — either the government or the military", also in [B30].

Banks and financial institutions may also become subject to espionage by attackers acting under government orders, like in the "persistent, months-long campaign that stole confidential info from Georgian government ministries, parliament, banks and non-profit organisations" [B33], where Russian security agencies were suspected as a source. Overall, the sophistication of certain malware used in digital banking attacks may suggest state involvement: "the geography of the targets and also the complexity of the threat leaves no doubt about it being a nation-state that sponsored the research that went into it" [B79]. This is also suspected for the case of the WannaCry malware that affected many organisations including banks throughout 2017 — in this case North Korea has officially been attributed as the originator by the UK and the US [336]. While exact details seem to be limited in the public domain, close monitoring of such actors seems required for banks and financial institutions.

There are other non-profit motivators behind digital banking attacks. Attackers may be looking for 'bragging rights' [B155] or be 'hunting for glory' [B55], showcasing their hacking skills to others through digital banking attacks. Similarly, attackers may deny criminal intent,

e.g. in [B18]: “motivated not by greed, but rather a love of computers and an ambition to be a software developer”, also mentioned in [B5]. In very rare cases, supporters of cybercrime (e.g. money mules) may not understand the criminal nature of their actions, e.g. in [B101].

Others may see themselves as helping financial institutions by highlighting previously unknown security vulnerabilities to them, rather than exploiting them [B55][B70]. A recent prominent example is the earlier mentioned case of T. Hunt exposing a vulnerability on the website of NatWest bank [337]. The publication of such vulnerabilities may be problematic for banks — they may have a negative reputational impact and encourage other attackers to exploit these vulnerabilities before they can be fixed.

4.1.10 Resources (funding and equipment)

The resources such as equipment and funding used by cybercriminals vary greatly, linked to the nature of the crimes committed as well as the set up and size of the group or individuals behind the crime. Most cybercrimes can be conducted using standard IT equipment, for example (high-capacity) laptops, mobile phones and hard drives: “police said they had confiscated two laptops, a tablet computer, a satellite phone and a number of external hard drives” [B9].

Malicious software tools purchased through internet channels are another resource frequently used by cybercriminals: “armed with $40 and a computer, an individual could easily get the Blackshades remote access tool and become a perpetrator” [B61]. These tools enable individuals to conduct crimes they would otherwise not have the technical ability for or support criminals to increase the frequency or potency of their attacks.

While many cybercrimes do not require special equipment, there are certain types of crimes that require specialised tools. To create physical credit cards from stolen or illegally purchased credit card numbers a number of tools are required, such as a “a vast quantity of blank credit cards, embossing machine and hot foil tipping machine, and a magnetic card reader used to manufacture cloned credit cards” [B150]. Other crimes against banks use inexpensive technical equipment like keyboard video mouse devices, which are used to take control over multiple computers in a branch, e.g. in [B100]. Additionally, ATM skimming also requires specialised (but seemingly readily available based on the amount (50) of references for this modus operandi in the sample) equipment such as cameras and physical skimming devices (which are placed on the card machine to extract card data), e.g. in [B271][B314].

While cybercrimes against banks can often be conducted at a relatively low cost and with limited manpower, DDoS attacks at scale are often suspected of having substantial backing, e.g. from national intelligence agencies, the military or other government-linked organisations — these case examples are however limited in our sample, e.g. in [B9][B79][B104], making this finding tentative and requiring further enquiry.

4.1.11 Skills

The cybercriminals observed in our sample display a large variety of skills, ranging from no specific skills (e.g. money mules) to highly knowledgeable individuals responsible for sophisticated and targeted attack campaigns — an overview is given in Table 4.2.

In our sample, attackers with no or low-level skills may be acting on their own accord or instructed by others. In the first case, they may often employ non-technical means, for example using insider access: "she noted down the information at work on a piece of paper" [B222]. Skills will be limited to basic usage of banking services and some individuals even claim not to understand the illegal nature of their involvement: "(she) had no knowledge of the overall workings of the fraud and got involved simply to earn a bit of quick cash" [B209]. Excerpts such as this one signify just how low the barrier of entry into cybercrime is at this end of the spectrum.

Most attacks against digital banking will however require some level of technical understanding and skills. Malware toolkits are a way to enhance these skills and enable non-coders to produce sophisticated malware including banking trojans [B13]. Users of these services may also benefit from customer services support [B142] and customisation produced for them.

However, many references in the sample hint at more advanced skills behind the attacks carried out. These attackers will be able to create their own customised code (or at least substantially amend existing code) to launch very targeted or large-scale attacks: "(he) wrote and polished the code for SpyEye until he had a product that experts described as professional grade" [B24]. Some attackers may also cover all stages of the attack and display quite a wide skill set: "(he) allegedly helped build the botnet that was used to direct the DDoS attacks, and authored attack scripts and created malware that were used to engage in the attacks" [B229].

Attackers targeting banks often not only possess skills to engage in attacks against services like online or mobile banking but may also target physical banking infrastructure and its underlying systems. Multiple attack vectors may be used for example against ATMs, including a "customised virus bought from a hacker forum" [B63] or infected USB sticks [B119]. While skills required may vary, it is likely that substantial technical background is needed to perform such attacks, as noted in [B119]: "the researchers added the organisers displayed 'profound knowledge of the target ATMs' and had gone to great lengths to make their malware code hard to analyse". Other examples requiring such technical skills include scamming attacks against card readers, e.g. the manipulation of existing machines by criminal Beeckmann in [B145] with his equipment showing "levels of sophistication not previously seen by investigators in this country (UK)".

At the top end of the spectrum for attacker skills, attackers are likely to display further skills beyond coding abilities — for example general attack innovation, strategies to hide their malicious actions (e.g. in [B109]), building and managing a criminal business model to support others in committing crimes (e.g. in [B43]) or large-scale, multi-stage attacks requiring substantial levels of planning [B42].

While the sample has shown a large range of skills present for digital banking attackers as

Attacker skills level	Skills description
Low	No specific skills, limited knowledge Malicious intentions
Medium	Toolkits, existing code Fraud-as-a-service users Social engineering
High	Advanced coding skills ATM, physical hacking skills
Extremely high	Attack innovation Multi-stage, large-scale attack campaigns Advanced criminal business model Operating under the radar without traces

Table 4.2: ***Overview of attacker skills levels***

shown in Table 4.2, it remains difficult to assign exact weightings to different skill levels within the sample. Proportionally, advanced and highly skilled attackers are in the majority in our sample, indicating an overall high skill level present in digital banking attackers with some outliers towards the lower (e.g. money mules, opportunistic toolkit users) and higher ends of the scale (e.g. coders able to produce highly targeted, destructive attack campaigns). And while the continuous advancement and availability of hacking tools has certainly lowered the barrier for aspiring cybercriminals (for example described in the report *Youth Pathways into Crime* [338] or [329]), the ongoing relevance of extremely skilled attackers in cybercrime has recently been highlighted by several unprecedented cyber heists against financial institutions (prominent examples include the attacker groups 'Odinaff' and 'Banswift' [339]).

While there is a lack of systematic assessments of attacker skills, official reports acknowledge the 'cyber arms race' between organisations, law enforcement and highly skilled attackers (UK NCA [329]). Ultimately, cybercriminals face similar challenges to corporate security teams: they will be looking for specific skills for the job to be completed (e.g. experience with DDoS, social engineering, cross-site scripting and SQL injection) in darknet recruitment calls (examples provided in [340]).

4.2 Group structures

This section describes characteristics of digital banking attackers in relation to community factors and group relationships. These characteristics include elements such as group size and characters, roles that attackers may have in a group and the nature of their relationships (between individuals and within groups). Table 4.3 shows an overview of the first level subcodes in this category — Tables 4.4 to 4.7 then show the lower level (second and third level) subcodes together with a brief explanation of the findings.

While examining the nature of the community attackers operate in as well as the relationships they maintain between each other and within their groups is certainly fascinating, certain limitations need to be acknowledged. Firstly, the codes included in the table do not necessarily represent all factors of interest when describing attacker communities or relationships, but

Codes (first level)	Sources	References
All in category code	188	838
Group size	112	201
Group character	66	171
Functions in group	101	253
Relationships	82	212

Table 4.3: ***Coding overview for group structures/community category code***

only the ones observed in the sample. Similarly, some codes, especially at a second or third hierarchy level, only have a small number of references attached (5 or under). This means that findings originating from these codes are only tentative at this point, pending further analysis (e.g. through addition of new data). While these limitations cannot be easily offset, related literature is referenced to help compare these findings where possible.

The section is structured as follows: firstly, the relatively well-defined elements of group size and functions held by attackers within groups are listed. This is then followed by some more tentative and explorative findings on the nature of the groups as well as relationships within or between groups.

4.2.1 Group size

A relatively easily identifiable factor in regard to community factors for digital banking attackers is the estimated size of the group they operate in. While this is only an indication based on a limited sample that should not be generalised, it helps to understand the attacking landscape digital banking is subjected to. An overview of the coding labels, their hierarchy and number of sources and references is provided in Table 4.4.

Code level				
First	**Second**	**Third**	**Sources**	**Refs.**
Group size			112	201
	Gangs and groups		67	107
		Very large	17	20
		Large	9	14
		Medium	15	24
		Small	33	47
	Lone attackers		22	25
	Only partial size known		21	23
	Unknown		43	46

Table 4.4: ***Coding overview for group size first level code***

The majority of attackers seem to be organised in groups of various sizes, ranging from small (groups of under 10 members) to very large groups (over 40 members), e.g. in [B255]: "Shaileshkumar P. Jain, along with his co-conspirator, Bjorn Daniel Sundin, [...]" or in [B97]: "police arrested five Ukrainians who were part of a 60-person group that used hosts in Britain to steal $70 million from US businesses". Again, it is difficult to verify whether these numbers are absolute, or groups are larger in reality. Overall, the relatively large presence of smaller groups is interesting, as is the high number of very large groups and lone attackers — while no dominant group size can be identified, this emphasises the observed variation between attacker groups.

No reference to accurate group sizes was found in the reviewed literature. In Chiesa et al. [93], lone attackers are seen as dominant, although demand for specialist capabilities for increasingly complex attacks is acknowledged as a reason for attackers to ultimately form groups. Forming alliances can provide the range of skills to overcome security mitigations in place and to truly work at scale to maximise profits.

4.2.2 Group character

This section outlines three attributes to characterise an attacker group:

1. *Cohesion* — loose collaboration to tightly knit
2. *Levels of sophistication* — in regard to group setup and overall organisation, low or medium to highly organised
3. *Hierarchy* — members of equal standing, no apparent hierarchy or undefined in contrast to strict or predominantly hierarchical setup

As these are the only categories that emerged through the grounded theory data analysis process, the overall numbers are fairly low overall (171 references from 66 sources in total) and mostly show varied results. Therefore, interpretations arising from this need to be considered carefully.

Firstly, the level of cohesion a group displays can range from a very loose collaboration with members on different continents, where group members do not know each other personally and only collaborate to benefit from each other, to a tightly knit group that works together daily and might be co-located or share other personal relationships (e.g. as friends or relatives). Many groups will also display different levels of cohesion within the group. While there is a core group directing the criminal activities, outer parts of the group may only be loosely associated — this is often the case when a group relies on a network of money mules, e.g. as mentioned in [B148].

It is also often difficult to measure the level of cohesion accurately — while it can be assumed that geographically dispersed networks are not as tightly knit as attackers in the same proximity, this is difficult to prove (16 references in Table 4.5). Text excerpt such as "chat logs from cybercrime forums [...] revealed he was conspiring with others from Russia, Lithuania and the UK" [B28] show a looser relationship, although additional data would be required to obtain adequate proof.

Code level				
First	**Second**	**Third**	**Sources**	**Refs.**
Group character			66	171
	Cohesion		43	56
		Loose collab.	15	16
		Tightly knit	18	18
	Sophistication/ organisation		43	73
		Low to medium	9	9
		Highly organised	32	33
	Hierarchy		40	42
		No hierarchy	21	21
		Hierarchical	21	21

Table 4.5: ***Coding overview for group character first level code***

Approximately the same number of references (18) can be found for tightly knit groups. This higher level of cohesion can be expressed in various ways:

- geographical proximity: living in the same postcode area or sharing a home, e.g. in [B150][B171] or [B206]: an alleged 'fraudster's utopia' in Harrow (UK);
- personal relationships: e.g. married in [B46][B185], wider family [B130][B147][B301] or friends [B54][B306][B316]; working for the same employer [B171][B187][B243];
- other factors, e.g. language like 'right hand man' to indicate a close relationship between two individuals [B168]; or
- sources may also directly describe the group in this way, e.g. in [B58]: "the government described Bogachev as a leader of a tightly knit gang of cybercriminals based in Russia and Ukraine".

The picture looks different for level of sophistication and organisation — here, a higher number of references indicate that these attacker groups are highly organised (32 references in Table 4.5). But how can levels be defined and measured? While these factors only provide an indication, the following aspects may be helpful to identify highly organised groups:

- scale and size of the group, e.g. large attacks involving many members [B92];
- level of organisation required to manage its members with an often corporation-like setup with clear division of labour present, e.g. in [B63][B88][B99][B103][B326];
- level of coordination and planning going into attacks [B74][B213];
- anti-forensics tactics built into attacks [B184]; or
- other sophisticated group setups, e.g. "only those proposed for membership by an existing user could join [...] the status of users determined who they could communicate with, and their access to commodities and services on offer" [B150].

Low to medium organised groups differ in the sense that they do not show these factors (or only partially) — in our sample, this may be examples of unsophisticated attacks (e.g. in [B222]: a bank worker writing down and passing on customer details) from small groups without a developed organisational structure, e.g. in [B150].

Lastly, roughly the same number of references suggest no or undefined (21) and a strict or defined (21) hierarchy levels. Hierarchy levels can be defined as an order present in the group, ranking its members according to their importance and authority. While no source document describes the complete hierarchy of a group, many references are made to some level of hierarchy in existence, e.g. "a senior position within the crime group's banking function" [B170], "a trusted position within the gang" [B195] or "the principal within this group of conspirators" [B135].

In summary, the following can be said for attributes of group structure as found in the sample. Firstly, the level of cohesion found within groups in the sample varies substantially. Even inside a group, different levels of cohesion may exist between subgroups and individuals. For sophistication levels, results suggest that most groups involved in digital banking attacks are highly organised to accommodate their complex attack campaigns — this is a tentative result however, as the number of references is limited. While the assessment on hierarchical structures in digital banking attacker groups has to remain open-ended, the presence of a hierarchy in many groups should be recognised.

4.2.3 Functions in group

As indicated in the last section, working together in a group can help to combine "unique and valuable skill sets" [235] of individual attackers. These powerful criminal alliances, or organised crime groups, are described in detail in *Cyber crime: understanding the online business model* from the UK NCSC [235]). Not unlike in a conventional company, for a group to be effective, a number of different, complementary roles need to be present. 12 different functions and roles can be identified for our sample (Table 4.6).

Most groups will contain a leading figure that leads on strategy: e.g. "the head of a fraud ring has been sentenced [...] he was the 'leader and prime mover', made almost all the calls" in [B163], with similar cases in [B10][B11][B15][B16][B23][B34][B135][B170][B187][B208][B312]. It is debatable whether group hierarchy and leading figures are observed in the same way by the attackers themselves and within their group as they are by investigators and prosecutors. Nevertheless, most groups will have a leading figure amongst their ranks and display some extent of hierarchy (also included in Section 4.2.2). There may also be variations of the theme, for example with a group of leaders in place [B10], attackers technically leading and 'masterminding' crimes with less of a management role [B24] or as key figures behind botnets [B19]. It is also worth noting that large groups may also have local leads to run the operations, helping global crime networks to separate into local groups and potentially diversify into other locations [B135][B154].

Similarly, groups need technical functions giving them coding and hacking skills, enabling various attack vectors via system intrusion [B54], advanced botnets and exploit toolkits

Code level			
First	**Second**	**Sources**	**Refs.**
Functions in group		101	253
	Botnet master/administrator	11	12
	Customer service	5	5
	Leaders	34	44
	Local agents	8	8
	Marketing and sales	13	18
	Money mules	35	61
	Multiple functions	8	9
	Other functions	17	21
	Recruitment	10	13
	Research	5	5
	Mentoring & enabling others	13	16
	Technical functions	31	39

Table 4.6: ***Coding overview for functions in groups first level code***

[B34], physical attacks against ATMs [B12] or creation of fake credit cards B115] or identity documents. Botnet administrators also play a significant role with a number of references in the sample (11 references in Table 4.6), for example the case of the large scale botnet run by Bogachev that also affected financial services and its users [B80].

Individuals in such roles may be part of the original group or recruited for their specific technical skills to fulfil a certain role or conduct a particular attack [B167] — this is also suggested in Leukfeldt [92] who sees new members recruited into groups constantly in response to new security measures (pp.89). Research to learn more about new security mitigations and eventually overcome these may be taken on internally by specialised group members or outsourced [B64]: "(they) had the job of finding out where fake bank cards, to be used with the captured PIN codes, could be produced".

Recruiting the right people for the job can give attacker groups a significant competitive advantage, e.g. in [B64]: "once recruited the hacker then customised a computer program specifically for the group, so they could use it to target bank accounts through ATMs". Overall, the relatively large number of references and variety of functions observed in our sample indicates that groups will likely have several different technical functions within their group (similar in NCSC [235]).

There are also a relatively large number of references related to money mules (alternatively 'runners' in [B264][B265] or 'cashers' in [B327]) — this is unsurprising and has been stated in prior literature on group structures (e.g. in Broadhurst et al. [233] and in Leukfeldt [92]), but it further corroborates the key role they play in digital banking attacks. The number of references encountered (61) is also likely to be owed to the large number of individuals required as money mules transferring funds through legitimate accounts to effectively launder the money and disguise its criminal origin (e.g. in [B301]). Money mules will usually be under strict instructions: "she'd just received notification that she was to expect a nearly $10,000 transfer to her bank account, and that she should pull the money out in cash and wire

the funds (minus her 8 percent commission) to three different individuals in Ukraine and Russia" (as told to security researcher B. Krebs in [B302]). While both terms may be used interchangeably, 'runners' as referenced in the sample will usually engage with the physical, offline side of scams and be tasked with support functions such as opening new accounts under false identity [B264][B265] or to extract the money ('cash out' [B92], 'cashers' in [B327] or local 'cash crews' in [B326][B329]). Several references also refer to mule recruiters or mule operators, as described in detail in [B101], where managing money mules is described as a sophisticated and organised undertaking requiring high levels of people management skills rather than technical abilities. While the sample does not provide detailed accounts of individuals working as money mules, the overall picture hints at a large number of involved individuals that are often the 'public face' of cybercrime likely to be caught before the group leaders working in the background [B173].

Additionally, a range of other roles can be found in the sample (see also Table 4.6) — while the overall numbers are lower, they are still interesting and provide further evidence to the high level of organisation, wide skillset and division of labour that can be found in attacker groups. Teaching, mentoring and enabling others certainly plays a role in our sample — this however does not usually take the form where more experienced attackers share their knowledge with novices for free, it is usually part of a business model. This instruction and ongoing support at a cost may take place through botnet provision [B19], toolkits [B86], crime-as-a-service or consultancy: "the gang moved into consultancy, helping to coach criminals [...] backed up by a web chat forum for an inner circle" [B43]. Other important activities included the marketing of services to other cybercriminals as prospective clients, e.g. in closed forums in [B76] or through social media in [B60]. Also, customer service is often offered for these services, e.g. in [B192]: "customer support via a dedicated Skype account". Other functions found in the sample include social engineers (e.g. in [B50]), money laundering (e.g. in [B19]) or other crimes such as identity theft, e.g. in [B43].

Similar to these findings, prior research on organised crime groups in general (not specific to digital banking) also confirms "substantial functional specialisation" (in Broadhurst et al. [233]). Others confirm this distribution of labour: in NCSC [235], both management (team leaders and money specialists) and technical functions (coders, network administrators, intrusion specialists and data miners) are outlined, while Leukfeldt recognises four positions in networks examined in his study on cybercriminal networks in [92] ch.6: core members, professional enablers, recruited enablers and money mules (as reviewed in Section 2.5).

In summary, digital banking attacker groups are made up of a variety of distinct skillsets and functional roles. However, it is also important to understand that groups and networks are flexible and may change over time (often around a fixed core group, as argued by Leukfeldt [92] ch.6) to accommodate new skill requirements, business growth or to engage in secondary criminal activities for example. Identifying the roles involved in a group helps to understand the business model underlying their crimes, with potential benefits for law enforcement and prosecution. While not all digital banking attackers are part of such an organised group, they form a central part of the attack ecosystem targeting financial institutions and its users — understanding that even non-technical roles such as money mules play an important role can help to devise comprehensive and cross-disciplinary security programmes.

Code level				
First	**Second**	**Third**	**Sources**	**Refs.**
Relationships			82	212
	Between groups		13	22
	Between individuals		62	124
		Character of relationship	39	55
		Interaction, communication	27	42
	Within groups		37	66
		Breaking trust	10	17
		Entry into group and gaining trust	22	34
		Subgroups present	13	15

Table 4.7: ***Coding overview for group relationships first level code***

4.2.4 Group relationships

Another aspect that can be used to describe groups of attackers are factors related to the nature of the relationship between individuals in groups of attackers, but also within and between groups. These can be factors examining levels of trust, communication and the nature of the relationship (e.g. online or offline). As with the factors discussed in Section 4.2.2, the overall number of sources and references at second code level is limited (with 212 references from 82 sources in total for this category in Table 4.7) — this will mean that any observations made need to be carefully examined and ideally be corroborated with insights from further related data. The observed relationship factors from the sample are now discussed in turn.

While the number of inter-relationships between different attacker groups are limited, several instances have been observed in the sample. Two types of interaction can be observed here: antagonistic, competitive behaviour and commercial collaboration. Competition and antagonistic behaviour can be observed between professional groups tasked to complete the same criminal task for profit (e.g. Chinese hacking teams in [B6]), but also between hacktivist groups (e.g. the two groups LulzSec and Team Poison in [B55]) for personal reasons or retaliation, although reasons may remain unclear to outsiders. Secondly, commercial collaboration may happen between groups (often summarised under the header of crime-as-a-service) where one group provides another with a service, e.g. large-scale fund extraction and money laundering services [B7], goods such as stolen payment card data [B62] or skills [B113].

For relationships between individuals in groups, an interesting aspect is certainly the presence of both online and offline relationships in the sample. While the crimes digital banking attackers engage in are mostly executed online, many references hint at an offline relationship, whether personal or purely for business reasons (as also discussed in Section 4.2.2). This

contrasts with references describing online channels such as forums (e.g. in [B221], similarly in [B188]) or instant messaging (e.g. in [B76][B221][B303]) as a way to communicate, start collaborating and form criminal groups (e.g. in [B25][B54]). This is in line with prior literature, e.g. in Leukfeldt ([92] p.98), where forums are seen as an important factor for growth of the group beyond offline social contacts, although this might not be applicable to all groups. Separately to that, while most individuals engaged in digital banking cybercrime seem to maintain several relationships with others, some attackers will state that they are working in a completely isolated fashion, e.g. in [B5] or [B29]: "(he) did not know anyone (involved in cybercrime) and did not intend to deliberately harm anyone".

Overall however, the assumption would be that most attackers have a range of relationships either within their attacker group or with other external collaborators to help conduct their attacks — while many of these interactions will be online as individuals are part of global attack initiatives or have collaborators abroad, a number of individuals know and work with each other on a face-to-face basis. This more nuanced approach to how cybercriminals work together, challenging the assumption that cybercriminals meet and work in cyberspace only, has recently been discussed in detail in Lusthaus & Varese [239] on the 'offline and local' nature of cybercrime, including the story of the 'cybercrime hub' of Râmnicu Vâlcea, a remote Romanian town (earlier described by Bhattacharjee in 2011 [341]). A related smaller-scale case can also be observed in our sample, where a cybercrime and fraud cluster in Harrow (UK) is described as a 'fraudster's utopia' by police forces [B206].

In the next two sections, factors related to relationships within groups are described, mainly around the internal structure of groups into subgroups and entering or leaving the group (based on building and breaking trust relationships).

Firstly, it needs to be noted that larger cybercriminal groups seem to have a complex setup with different functional parts, subgroups and varying levels of cohesion (as discussed in Section 4.2.2). Several references in the sample demonstrate the split into subgroups and separate functions — this may take forms similar to departments in lawful corporations [B101][B170]. Other ways to separate business areas from each other is based on geography, where large gangs will have different arms in different countries [B166]. Hierarchical order can also be used to split groups, e.g. with money mules as a subgroup lowest in the hierarchy in [B143]. This will also mean that parts of a group might be caught and prosecuted separate from the rest of the group, e.g. in [B53][B168].

Lastly, how can individuals become members of groups? Trust seems to play a large part in this in our sample. Potential collaborators may be recruited directly into a group if the leader trusts them, e.g. as relatives, friends or other trusted business contacts [B147][B181][B316]. This may also take the form of individuals meeting online without previously knowing each other — in this case, other trusted intermediaries may be able to vouch for an individual's criminal potential and skills, but also for reliability when working together: "this is the central paradox of this marketplace. In order to get in, you have to be a verified credit card thief. But in order to do business, you have to show that you can deal honestly" [B32]. Another way to establish trust between cybercriminals, especially if they initially met online [B54][B116]) is through continuous collaboration around criminal activities. Additionally, individuals that can demonstrate "skills and achievements that could contribute to the criminal community"

[B195] may also receive right of entry to a group — this is acknowledged in detail in prior literature in Chiesa et al. [93] p.162 as 'initiation rites'.

But trust can be a fragile thing in groups of cybercriminals: in [B119], "the crimes' masterminds appeared to be concerned that some of their gang might take the drives and go solo" and build in an extra authentication layer — for their own group members. In [B121], individuals in the groups turned against others, handing them in to the police. Similarly in [B55], an alleged retaliation act was conducted for 'snitching' on others: working with the authorities will most certainly break levels of trust established.

4.3 Geographical distribution

This section is concerned with where attackers in the source materials attack from — an overview of references found in the sample is provided in Table 4.8. While not necessarily a focus in the attempt to define digital banking attacker characteristics, it is nevertheless a notable part of an attacker's profile: it is assumed that geographic attributes can ultimately help to create a rounded and complete character representation or persona.

There are several issues to consider when looking at individual countries as attacker origins, especially when working with a finite sample which inherently does not fully represent the entire community of attackers. Firstly, the source material will strongly define the distribution of countries within the sample, potentially creating a bias due to the relatively limited sample size (>300 cases) and geographic focus of the original datasets (e.g. UK-centric in [34] or US-centric in [36]). A further issue may be the timeframe (2010 – 2019) underlying the source material — the constant change and development over time in cybercrime may mean that countries as major attack sources will fluctuate and change over time. A further complication is introduced by the chosen focus on digital banking only: no comparable large-scale statistics describing geographic factors for this particular set of attackers seem available at this point in time, hindering a meaningful comparison and potential validation of our data against existing literature.

For these reasons, results from the sample are therefore presented in Table 4.8 in a largely descriptive manner with limited explanatory power. A number of interesting external resources (usually from global security vendors) describing attack origins, although not specific to digital banking, are available for reference in this context; for example based on the geographic origin of attacks on dedicated honeypot networks (in e.g. Deutsche Telekom attack sensors [342] or statistics from the Honeypot Project [343]) or originating IP addresses for attack traffic on client networks (in e.g. Akamai *State of the Internet* [344] or LexisNexis ThreatMetrix [345]).

While the geographic distribution of digital banking attackers can not be generalised from the limited sample in use, another noteworthy aspect to mention emerged from the data at this point: the humans behind this type of cybercrime appear to be an exceptionally mobile group across borders. When examining the origin and location of usual residence of cybercriminals in the sample, one cannot overlook a behavioural pattern shown by many individuals in this group: they travel and move countries extensively, with some of them

Codes (first level)	Codes (second level)	Sources	References
All in category code		235	658
Africa		16	18
Americas		64	147
	Canada	8	23
	Caribbean	1	1
	South America	15	56
	United States	48	66
Australia/Oceania		11	14
Asia		42	69
	China	13	22
	India	6	14
	Middle East	12	16
	Rest of Asia	11	14
Europe		179	336
	UK	113	149
	Western Europe	23	31
	Eastern Europe	57	73
	Russia	37	51
	Ukraine	21	33

Table 4.8: ***Coding overview for geographical distribution category code***

also captured or convicted in other countries. This is evidenced in the sample by 75 text excerpts coded under the headings of 'extensive travel/multiple locations', 'different country of capture or conviction' or 'foreign nationals operating abroad'.

Profiles in the FBI Cyber's Most Wanted list [36] offer some useful examples of individuals with multinational ties and a high potential for cross-border travelling: "Belan has Russian citizenship and is known to hold a Russian passport. He speaks Russian and may travel to Russia, Greece, Latvia, the Maldives, and Thailand" [B218] or "Aaron has ties to Maryland and Florida in the United States; Tel Aviv, Israel; Kiev, Ukraine; and Moscow, Russia. He may travel to any of these locations or to other locations throughout Eastern Europe" [B236] and "Jain is a United States citizen who has ties to Brazil, Canada, India and the Ukraine" [B246]. Other examples in the sample include the previously mentioned Blackshades co-author Yucel — originally from Sweden, he collaborated with others worldwide and was arrested in Moldova to be extradited and convicted in the US [B142].

While not explicitly evidenced in the sample, it can be assumed that the reasons cybercriminals choose certain locations as a base (and subsequently change them frequently) are down to personal preference (e.g. Spain or Dominican Republic), to enable them to carry crimes out in certain countries, use local expertise through locally based agents or simply to escape from the authorities and avoid being extradited or convicted. This transitional and mobile nature of cybercriminals is also evident in the cross-border collaborations and relations that many cybercriminal gangs will display. They will work together across borders with other criminals of different nationality if they can benefit from this: "what makes money in Russia today, could be used in attacks against American users tomorrow" [B57].

Depending on the specific nature of the cybercrime carried out, large gangs will often rely on local or international agents to help execute their crimes, especially when it comes to extracting or laundering the illegally obtained funds (e.g. the synchronised mass withdrawals from cash machines all over the world in the WorldPay heist [B85]). This set-up can also be observed when investigators start 'following the money' — in extreme cases such as the Liberty Reserve money laundering fraud, "tens of millions of dollars" are moved through multiple layers of international accounts and "through shell company accounts maintained in Cyprus, Russia, China, Hong Kong, Morocco, Spain, Australia and elsewhere" [B91].

The truly international nature of cybercrime and its actors calls for cross-border investigations and international collaboration on the law enforcement side — there are certain examples where coordinated raids, arrests and convictions were conducted, e.g. for the case of Blackshades, where "the UK's NCA said 15 arrests took place in England and two men were held in Scotland. 80 others were held in 15 countries including the US, France and Germany. Further arrests abroad took place in Moldova, Switzerland, the Netherlands, Belgium, Finland, Austria, Estonia, Denmark, Canada, Chile, Croatia and Italy" [B13]. This part of law enforcement certainly remains difficult, e.g. through differences in local laws or lack of mutual agreements in place — this is further discussed in Section 5.3.

4.4 Key points and summary

Given the length of this chapter and the amount of observations listed, a presentation of key points seems warranted at this point. This is then followed by a reflection on currently perceived limitations, an outlook on potential next steps and further research stemming from these results. Based on the findings presented in this chapter, the following statements summarise the key findings on characteristics of attackers targeting digital banking systems from the grounded theory analysis of our sample. While these statements only provide a generalised overview of the findings, it is hoped that they capture the most significant and remarkable findings.

1. *Globally transient, moving and collaborating across borders* — the truly international nature of cybercrime enabled by the global reach of the internet also presents itself in its actors, which may often physically move between countries or (virtually) collaborate with other attackers based abroad.

2. *Varied range of resources and skills* — equipment and funding (resources) used by attackers vary greatly and is often dependent on the setup and size of the group or individuals behind the crime. Somewhat surprisingly, cybercrimes against banks can often be conducted at a relatively low cost and with limited manpower. Nevertheless, many attackers and groups show a significant level of resources and funds. Most attackers exhibit advanced to very high skills and technical capabilities, although less skilled attackers and supporters (e.g. money mules or toolkit users) can be found.

3. *Financially motivated, although several other non-profit motivators exist* — the motivation behind digital banking attacks and for its attackers is primarily profit; ranging from individuals 'making a living' to earning significant wealth from their criminal ac-

tivities against financial institutions. Non-profit motivations lie mainly in the areas of cyber activism and terrorism or nation-sponsored attacks, but there are a few cases where attackers act mainly for the challenge well-protected banking systems pose or to point out vulnerabilities.

4. *Young (but not very young) and male* — the average for attacker age in our sample is just over 30, with most individuals aged between 21 to 35, although several teenage and much older individuals as outliers in the sample exists. Secondly, attackers are predominantly male (under 10% of individuals are female where stated).

5. *Varied range of education levels and occupations* — attackers show a wide range of formal and informal education levels and can be found in a variety of occupations and professions. This is likely to be because of the many facets of cybercrime against financial services, the various paths into cybercrime and the roles to fulfil. Occupations of attackers roughly fall into four categories: not related to banking or IT, IT in its widest sense including security, financial services and professional criminals.

6. *Recruited through online channels* — cybercrime networks grow through recruitment efforts — this may be through social contacts, but it is likely that online channels (targeted through hacker forums and chats as well as social media in general) play a significant role in regard to the entry into cybercrime.

7. *Prepared to do harm to others with few moral concerns* — attackers willingly accept the harmful consequences of their actions and often have no issues purposefully targeting vulnerable members of society if this is to their advantage. However, some individuals may feel remorse or have an unconventional idea of morals, values or sense of justice.

8. *Just like everyone else, but not quite* — attackers are not necessarily different from other populations of individuals — they may lead a relatively normal life with their family for example. In strong contrast to that, attackers may also be vulnerable individuals finding themselves in difficult personal circumstances that force them into cybercrime.

9. *Stronger as a group, even if it is small* — while not all sources state the size of a group, most attackers seem to be organised in groups, ranging from small (under 10 members) to very large groups (over 40 members). No dominant group size can be identified with a large variety present. It is notable that a relatively strong presence of smaller groups is evident, but there are also very large groups.

10. *Various degrees of cohesion and hierarchy within groups* — attackers organised in groups may be part of loose collaborations or tightly knit groups. The level of cohesion varies across the sample. Even within the same group, different levels of cohesion may exist between subgroups and individuals (e.g. money mules may be a largely separate entity to other parts of the group). Similarly, levels of hierarchy encountered within a group may vary from non-hierarchical to strictly ordered by seniority or authority — again, there may be differences in hierarchy levels between different parts or subgroups.

11. *Highly organised, adaptive and multi-skilled* — many groups in our sample are made up of a variety of distinct skillsets and functional roles. Additionally, groups and networks can be seen as flexible and may change over time to accommodate new skill

requirements, business growth or to engage in secondary criminal activities (tentative suggestion in sample data, but in line with previous results, e.g. in Leukfeldt [92]).

12. *Online and offline relationships matter* — attackers in the sample seem to be well networked with a range of relationships within their attacker group or with other external collaborators to help conduct their attacks — these communications often take place online, but also offline and locally.

13. *Trusted to be criminal* — trust plays a central role for collaborations between attackers and for group entry, with only trusted individuals recruited into groups. Trust can also be built through intermediaries 'vouching' for others, their skills and criminal intentions — this can also be achieved by showcasing skills and attacks to others. Lastly, trust can break easily if others act suspiciously (e.g. potential 'snitching' to authorities).

This list is in contrast to several attacker characteristics that are currently not included in further detail in our results, mainly because of a lack of references in the source material for these items.

- *Detailed geographical distribution* — although a wide geographical distribution of digital banking attackers is indicated in our limited sample, with attackers based in a range of countries including the US, China, the UK as well as Russia, Ukraine and Eastern Europe, the finite nature of the original dataset with its focus on certain countries makes meaningful interpretations difficult. Reports on geographic attack origins are widely available in the public domain as included above, however not for the specific case of digital banking. Data derived directly from financial institutions could potentially help to close this gap in the future.

- *Psychological traits of attackers* — the method used and source materials have not yielded sufficient data to gather findings regarding psychological traits of attackers, including their level of self-esteem or self-centredness (e.g. in Chiesa et al. [93] pp.102 and also discussed in Ziegler & Fötinger [140] pp.19).

- *Further personal details* — beyond what has been mentioned in Section 4.1, not many personal details about attackers are known, e.g. their exact personal circumstances or family background, but also non-attack related details like their non-criminal past or preferred leisure activities.

- *Group dynamics* — while some key aspects on groups are covered in the findings and the interesting observations in regard to intra-group relationships have been noted, further details on group dynamics remain hidden due to a lack of relevant data in the sample. This aspect has been addressed in depth in the work of Leukfeldt in [92] on cybercriminal networks.

- *Self-perception of attackers* — due to the secondary, indirect data collection not involving interviews with digital banking attackers, no data regarding how digital banking attackers view themselves is currently available. This also stretches to other aspects important to the individuals, for example how they view their criminal careers overall and what their perspectives for future life look like. Chiesa et al. [93] pp.91, and Thackray [94] have provided some insights into this topic, but without a digital banking focus.

- *Lack of some very recent cases and developments* — due to the timeframes and geographical focus of the datasets used, several recent developments and prominent individual cases may not have been included. An example could be the potential impact of the COVID-19 pandemic on general contingency planning, but also threats from rising levels of cybercrime, for financial services institutions (as advised by the European Central Bank Supervisory Board in March 2020 [346].

Based on the summary of gained insights and the gaps outlined in this section, several next steps and further research directions can be identified. Firstly, all aspects related to attack-related behaviour (modus operandi, preferred targets and jurisdiction factors) that have been coded and identified during the analysis process (as outlined in Section 3.4) should be enumerated and reflected on — this is done in Chapter 5. Once these additional analysis results have been collated and presented, there is the option for meta-analysis of these results. One example of such an expansion is the creation of distinct groups of attackers, following the example of an attacker typology as introduced in Section 3.5.2 — this is attempted in Chapter 6, and further extended through the visualisation option of attacker personas in Chapter 7. With all this information on attackers in place, the potential benefits of collecting and analysing such information in security practice are of interest — this is part of Chapter 8.

Very few people are aware of the extent of the online criminal ecosystem that supports and enables cyber attacks, and the business model behind it.

— Matt Carey,
Head of London Operations Team NCSC
2017 [235]

5

Attack-Related Factors and Behaviours

This chapter describes the analysis results regarding attack-related aspects and behaviours shown by digital banking attackers in the datatset examined. This includes preferred targets, common modus operandi and factors relating to investigation and prosecution of cybercrime incidents. References to previous literature are added where possible and deemed useful. A dedicated section summarising and reflecting on these findings is provided at the end of this chapter.

In continuation of Chapter 4, this chapter is structured using headings that directly follow the code structure as it emerged throughout the data analysis phase (compare to Figure 5.1). Firstly, aspects in relation to targets selected by attackers, such as their geographic distribution, monetary damage caused to these targets and notes on their selection, are described. This is followed by a brief treatment of the common modus operandi behind attacks against digital banking, including standard attack vectors and other means supporting such attacks, but also perspectives on the overall business model and the level of risk that attackers are willing to take. Lastly, characteristics of cybercrime investigations, including charges and sentences, as well as factors positively supporting (or hindering) an effective prosecution process are remarked on.

While the contents of this chapter focus primarily on the attack itself rather than the attacker (in contrast to the previous Chapter 4), most parts of this chapter are still closely related to attackers and their behaviours and can be viewed as useful in the context of attacker categorisation, profiling and representation (as picked up on in Part III of this thesis). This

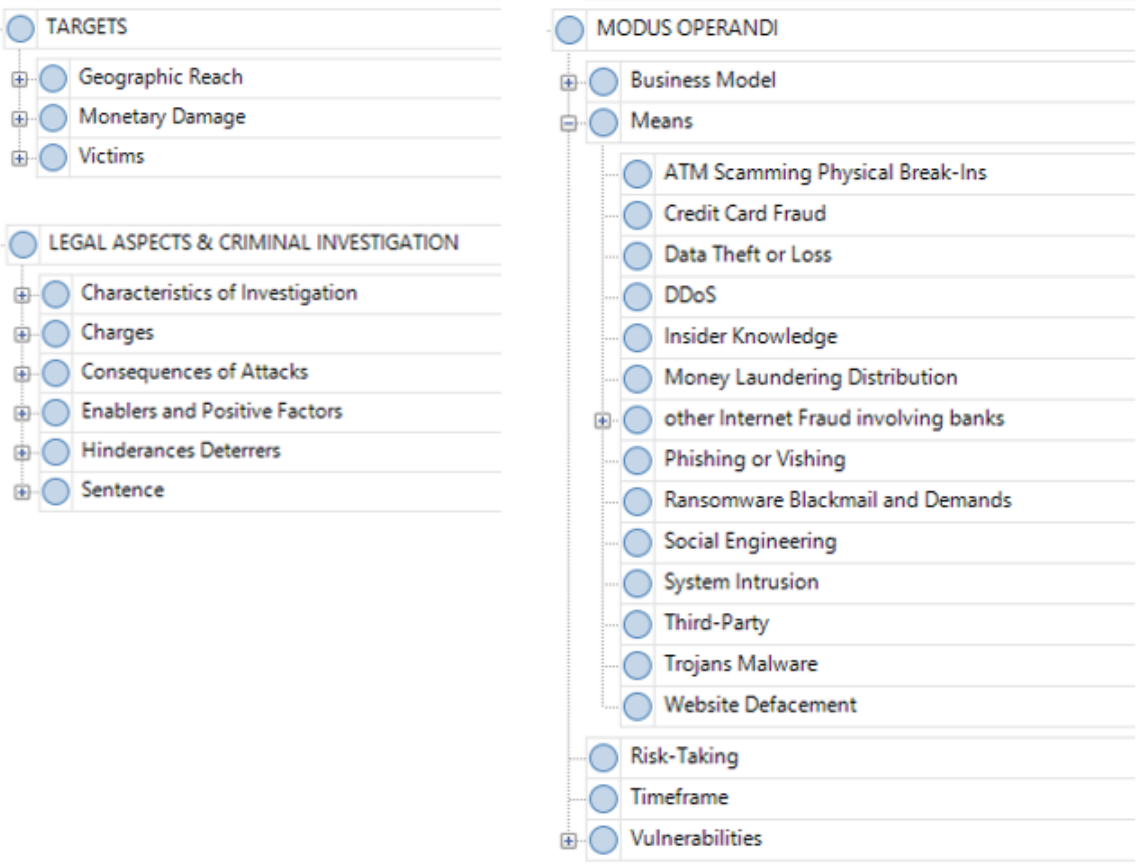


Figure 5.1: ***Emerging code structure from data analysis (attack-related factors)***

assessment slightly varies for the third element discussed in this chapter: observations regarding legal aspects and criminal investigations as found in the original dataset. While aspects coded under these headings are not necessarily related to individual attacker characteristics and behaviours, they form part of the overall analysis and may provide some useful insights for future research and are therefore included.

To maintain a close relationship and grounding with the original dataset analysed, individual sources from the examined dataset are referenced and listed alphabetically in Appendix B, following the format (e.g. [B123]) explained and used in the previous chapter. Following the structure of Chapter 4, any references external to the analysed dataset, for example to related academic or commercial literature, are included in the standard bibliography at the end of this thesis.

5.1 Targets

This section describes characteristics related to targets selected by attackers. For the examined dataset, these fall into three main categories: geographic reach of the attacks and distribution of targets, overall monetary damage and selection of targets and those affected (for a definition of the term 'victim' as used in the context of this work, refer to p.103 in the previous chapter). Table 5.1 shows the codes for these categories down to the second code level.

Codes (first level)	Codes (second level)	Sources	References
All in category code		172	480
Geographic reach		53	127
	Multiple countries	34	57
	National	14	16
	Affected systems	25	50
Monetary damage		107	144
	Under 1 million (£/GBP)	28	31
	1 to 100 million (£/GBP)	62	81
	100+ million (£/GBP)	11	14
Selected targets and victims		107	209
	Financial institutions	43	62
	Other organisations	33	70
	Individual users	45	54
	Specific reason for selection	12	15

Table 5.1: ***Coding overview for targets category code***

5.1.1 Geographical reach of attacks

Interestingly, the number of codes in this category is lower than the number of codes explaining the geographical distribution of attackers (compare to Section 4.3). There are several explanations for this effect: either this information is considered less interesting to readers and hence not reported, or this information is simply not known and cannot be included. While an attribution to individual countries as attack targets proves difficult due to the limited case numbers specifiying this information in our sample, the following general statements can be made. Although most attacks seem to target multiple countries, a substantial number of nationally focused attack campaigns can also be observed. Furthermore, the number of systems (computers or ATMs) affected by attacks is very significant — a number of references recording over 1 million compromised systems can be found, e.g. in [B7] or [B64].

In our sample, attacks will be targeting a variable number of countries. Some may only target a few selected economies: e.g. in [B184]: "primarily targeting elderly and vulnerable US and UK victims". On the other hand, cybercriminals may decide to target a larger number of countries ("[...] a sophisticated phishing scam to access the accounts of bank customers in 14 countries" [B151]) and others will target users worldwide, e.g. in [B9][B61]. While there are some purely national cases with cybercriminals based in a certain location targeting only users from this economy (e.g. [B21]), most attackers seem to 'cast the net' as wide as possible and expand their criminal activities to as many countries as feasible to achieve maximum returns. This is also visible in the coded references under 'number of systems affected': significant numbers of computer systems can be compromised through large botnets (e.g. Bamital: 8 million computers in 2 years or 12.7 million assumed for Mariposa [B8][B19]).

It is worth noting at this point that there are limitations to global targeting, e.g. attacks involving social engineering methods relying on local language skills or the presence of local 'cash crews' to extract funds at their origin. Such reasons for the selection of targets are

discussed in more detail in Section 5.1.3. Overall, no distinct patterns can be recognised regarding strategies for selecting geographies to target — in line with the many different types of attacks present, a large variety of geographic target strategies can be observed across the sample.

5.1.2 Overall monetary damage

The aspect of monetary damage caused by attacks in the sample is one of the few quantitative variables analysed in the sample. These numbers generally describe the overall, total monetary damage rather than losses suffered by individuals. Furthermore, as the sample is limited in the number of cases, the results presented here only give an indication of the negative monetary impact that individual attackers or groups of attackers may have. To help put these numbers in perspective, statistics on cybercrime losses are added for reference later in this section.

For the actual losses encountered through individual attack campaign attacks in the sample, numbers appear substantial even at the lower end of the scale (under £1m[48] category as included in Table 5.1), with examples ranging from £2,600 [B205] to £770,000 [B33]. The average in this lower category of monetary damage caused by attackers by the time of their conviction amounts to just under £300,000 (approximately £296,642; over variable timeframes ranging from one single attack to ongoing attacks spanning several years). Most overall monetary damage caused is however significantly larger: for the bracket of up to £100 million, 81 references (from 62 source documents) are recorded — most losses seem to lie within this range, with the average across the coded references around £12.6 million. There are however also individual cases with much higher assumed losses (£100+ million), for example through attack vectors such as botnets (e.g. in [B105]), large-scale phishing and credit card fraud schemes (e.g. in [B52] and [B72]).

There are several cautions around these numbers. As mentioned, different timeframes are used in the data sources, making it difficult to compare these numbers. Also related to the data sources, it is not always clear what kind of crimes are covered under the losses stated, whether these are all related to crimes in the area of digital banking and how much money was actually lost and subsequently not recovered [B139][B200][B261]. Many sources are also vague in regard to the exact amounts lost, describing losses with terms such as 'millions' rather than exact monetary figures, e.g. in [B176] or [B326].

Another detail missing from the data sources are losses to individual users — only aggregates are provided here, e.g.: "a gang of fraudsters have been jailed for between 21 and 64 months for stealing bank card details potentially worth up to £16m from more than 60,000 people in the UK and abroad" [B197]. Despite these considerations, monetary damage in the sample varies greatly, but appears very significant — even individual attackers and smaller groups seem to show potential for causing significant harm.

[48]British pound sterling (£/GBP) is used as a reference currency in this section, although losses may also be denoted US Dollars and Euros in the sample — an approximate currency conversion rate where 1 GBP equals 1.33 USD and 1.18 EUR (December 2019) was applied.

The overall average financial cost of incidents is given as £857,000 by PwC in 2018 [347], based on a sample of organisations reporting their direct losses — the average value in our sample (where exact values are given in the references) however is higher (closer to £10 million[49]). This might be due to some larger outliers above £50 million, but could also be due to a financial services focus in the sample, which may mean the cost of cybercrime is higher than in other industries (in [349]). Damage affecting individual customers is not immaterial either. In the UK, the average loss for individual cybercrime victims was given as £523 across all cybercrime types, although certain types might be signficantly higher (e.g. financial investments fraud at an average of £32,000 loss; both figures from UK Action Fraud for 2017 [350]).

For financial services organisations, a model provided by cyber insurer Lloyd's of London shows large to even extreme losses for an example scenario of a cloud service provider outage due to an attack (from $1.29 billion up to $16.72 billion in [351]) — this certainly highlights the vast financial damage and devastating effects cybercrime may theoretically have on organisations. Finally, the true cost of cybercrime is even more difficult to quantify: in addition to direct financial losses, reputational and long-lasting brand damage due to encountered cyberattacks may severely harm a business for a prolonged period of time. An example is the case of customer data theft (credit card and personal data) suffered by British Airways and directly affecting customers of the card-issuing banks in the UK — while difficult to measure currently, the reputational impact and losses in bookings may be higher than direct financial losses [352].

5.1.3 Selected targets and victims affected

Naturally, for a dataset focusing on digital banking cybercrime cases, most observed targets will fall into the category of financial services. However, other organisations affected are mentioned in the sample, which are briefly discussed in this section. Unfortunately, reasons for the selection of specific targets are limited in the sample (as visible in Table 5.1). Due to this low number of observations, results in this context can only be considered as tentative and requiring further verification. Finally, the impact of cybercrime on individual users and banking customers as victims as observed in the sample is discussed in this section, including a brief note on liability for fraud losses in this context.

Many targets in the sample are retail banks and their personal customers, including examples such Santander, Royal Bank of Scotland, Clydesdale and Yorkshire Bank in the UK, Postbank in South Africa, several German institutions and US banks, e.g. First National Bank Omaha, Union Bank Lincoln [B87][B111][B138][B179][B213]. In a number of examples, banks are not identified by their name, e.g. "online criminals have targeted a top European bank, stealing more than £400,000" [B141]. There are however also some examples of business customers in the sample, e.g. the attacks against RBS WorldPay [B85][B326].

[49] Counted across the entire sample with 85 occurrences, with 5 outliers removed — this concerns values of almost a billion US dollars in e.g. [B72]. Florencio & Herley have acknowledged the distorting effect of single outliers in their critique of cybercrime surveys in [348], together with issues such as unverified self-reported numbers and small sample rates, confirming the indicative nature of figures in this context.

Other than banks themselves, the sample also includes other payment providers and suppliers that have fallen victim to cyberattacks. Payment providers such as Visa, MasterCard and PayPal have been subject to attacks [B209][B218] — for example in past attacks by the online activist group 'Anonymous' against these organisations in support of Wikileaks in 2010 [B10]. For third-party suppliers, the example of an Indian card processing company can be observed [B7] in the sample, as well as a trading software for stocks and securities [B35]. This stresses the importance of analysing and identifying threats to the entire ecosystem of a bank, including external third parties (also in [B269] or [B320]).

Furthermore, a number of organisations outside banking have been named as subjects of large-scale attacks in our sample. These include government departments [B79][B121][B191][B327], non-profit or academic institutions [B15][B45][B79][B192], but also internet-based companies including web hosting providers, online retailers, social media companies, start-ups or gaming providers [B27][B80][B120][B190].

How then are these targets chosen by cybercriminals? Two elements are likely to be overarching motivations for attackers: target attractiveness and opportunity, as reflected in this statement in the sample as to why the EU will remain a key target [B58]: "because of its relative wealth, high degree of internet penetration, its advanced internet infrastructure and increasingly internet-dependent economies and payment systems". More specifically, individual attackers may choose their targets based on perceived weak defences, for example small businesses [B126] or vulnerable customers, e.g. individuals who "had fallen on hard times and were looking for loans over the internet" [B205] or "the elderly" [B311]. Technical problems at banks may also offer attack surfaces, e.g. through phishing emails appearing as genuine support messages as reported in [B292].

Existing specialist (or insider) knowledge giving attackers an advantage might also play a role in them selecting their targets, as might world events or political developments for online activist groups [B123]. Lastly, one source [B126] remarks that "doubly concerning for many organizations and executives was that target selection by these groups didn't follow the logical lines of who has money and/or valuable information", showing that while most attackers choose their targets for specific reasons, some might be more unpredictable. But attackers might not only choose targets actively, but also avoid them for a number of reasons: attackers may opt against attacking users in their own country (e.g. Russia in [B109]) or avoid critical infrastructure or law enforcement agencies [B104].

Careful selection of targets is crucial for attackers and their planning: attacks may require specific and localised preparation efforts, e.g. money mule recruitment campaigns [B101]. The selection of targets may also influence the attack strategies attackers may employ, e.g. exploiting human vulnerabilities through social engineering or phishing to overcome perimeter protection in larger companies [B126].

Information on individual users as victims is limited in the dataset. However, one of the key insights is the vast number of potentially affected users in many attacks in the sample, e.g. in [B246]: "internet users in more than 60 countries", "personal details of almost 30,000 bank customers" [B151] or "750 RBS customers" [B161]. While many, if not almost all, internet and online services users face some risk to fall victim to cybercrime, it seems to be that

some users are more vulnerable than others, e.g. those less able to protect themselves (due to lack of knowledge or with the inability to pay for protection, as in [B99] or in [B311]). Some attackers may even use so-called 'sucker lists' for individuals likely to fall for repeat social engineering scams [B184]. The individual impact on victims may vary, but can have a devastating impact on people's lives, as described e.g. in [B148]: "a phishing attack that netted them a woman's £1 million lifesavings" or in [B174]: "one victim alone was defrauded of over £2 million".

This potentially enormous impact on a large number of users naturally raises the question of liability: who is responsible for these losses and will ultimately cover them? Unfortunately, not many sources in the sample refer to this aspect. Where discussed, banks or credit card companies will cover any losses encountered by their customers as a result of cybercrime, e.g. in [B14] or [B115]: "Australian banks and credit unions have reimbursed the $30 million to the 30,000 Australians whose details were exposed by the hacking gang"). Some level of controversy around shifting liability from financial services firms to their customers prevails, with cases of banking customers being deemed liable due to gross negligence or for authorising the fraudulent payments (usually based on case-by-case review procedures different for each bank, e.g. in [353]; refer also to Anderson et al. *Measuring the Cost of Cybercrime* [354] and updated in [355]).

However, the current status quo in the banking industry is that cybercrime losses are mostly covered [356], with the FCA in the UK also recently attempting to strengthen victim protection around certain types of fraud (refer to Section 2.5.2), with banks also passing on their cost to third-parties such as suppliers, payment providers or insurance companies [354]. This seems to be the case at least in the UK and the US and might differ in other legislations: e.g. in India, the very limited customer protection in the case of fraud is currently under scrutiny of the central banking institution [357]. Given the vast cost of cybercrime and card fraud, this controversy can be expected to continue (also in [B99]) and could become a "battleground for liability claims between banks and their customers" [356].

5.2 Modus operandi

This section provides a summary of observations made in the dataset regarding the modus operandi behind attacks targeting digital banking systems. The first part presents a list of attack vectors and other means supporting attacks as well as a brief note on timeframes of attacks and exploited vulnerabilities where known. Another variable present in the dataset that helps to describe the modus operandi underlying attacks against digital banking systems is the business model employed by cybercriminals. Lastly, several observations on the level of risk-taking in attackers are made.

5.2.1 Employed attack vectors and supporting means

The following categories of high-level attack vectors for attacks targeting digital banking systems can be identified from the dataset (refer also to Table 5.2).

Codes (first level)	Codes (second level)	Sources	References
All in category code		251	657
Attack vectors		227	476
	ATM, physical break-ins	37	50
	Card-related	23	34
	Data theft or loss	26	34
	DDoS	32	43
	Insider knowledge	43	57
	Money laundering	21	33
	Other online fraud	27	34
	Phishing or vishing	19	22
	Ransomware & blackmail	3	4
	Social engineering	30	44
	System intrusion	18	23
	Trojans and malware	54	84
	Website defacement	6	7
Business model		35	71
Level of risk-taking		22	25
Timeframe		32	35
Vulnerabilities leading to attacks		37	50

Table 5.2: ***Coding overview for modus operandi category code***

- Trojans and malware (84 references)
- Social engineering and human targets (44 references)
- DDoS attacks (43 references)
- ATM-related and physical break-ins (50 references)
- Card-related (34 references)
- System intrusion (23 references)
- Phishing and Vishing (22 references)

While this list provides a baseline list of attacks, the current situation of digital banking attack vectors can be expected to continuously evolve. To compare the results derived from our dataset (which covers approximately the last decade, as described in Section 3.4) to the current position, brief reference to current literature is made here.

When looking at trend forecasts by security vendors specific to the financial services industry for the years 2019 and 2020, attack levels are expected to remain at a high level, also expanding to the supply chain of banks such as technology providers, exchanges or payment providers [358][359]. Kaspersky Lab support this aspect by viewing online payment processing systems for e-commerce systems as a direct target for attackers in the near future, essentially bypassing banks' security mechanisms, but still affecting their customers [360] — a further rise in attack patterns against payment operations including SWIFT, but also physical infrastructure such as ATMs is predicted by researchers at F-Secure [359]. Large

scale DDoS attacks, but also targeted ransomware attacks are viewed to remain prevalent [360], with state-sponsored attackers also relying on these attack vectors [359]. New variants of mobile banking trojans are seen as on the rise by Kaspersky Lab, following the publication of the source code of several popular trojans [360] — Trendmicro also state a continued risk in attacks targeting SIM cards (e.g. when used as part of customer authentication solutions) through social engineering [358]. But attackers may also decide to rely on existing attacker vectors including malware and shift their efforts to new targets such as fintech and investment applications [360] as these may not use the same level of best-practice security as banks (such as multi-factor authentication).

A number of means directly supporting attacks can be identified as relevant to digital banking attacks in the analysed sample.

- *Money laundering and cash extraction* — one of the key aspects of digital banking fraud are money laundering procedures (for example through moving money rapidly through legitimate bank accounts under the control of organised crime groups) as well as the physical cash extraction as the last stage of the attack, usually carried out by local money mules or cash crews, e.g. [B143][B155][B166][B200]. 33 references in total identified in sample.
- *Insider knowledge* — several digital banking fraud incidents in the sample have been supported by insider knowledge, e.g. call centre employees stealing and passing on customer details [B213] or a bank worker conspiring with criminals to steal money, giving them access to the bank's system [B160]; also in e.g. [B181][B201][B206][B268][B299][B311]. 57 references.
- *Other types of fraud, including identity fraud* — as digital banking fraud often relies on the ability to access standard bank accounts, supporting fraud types may involve signature (e.g. in [B163]) and identity fraud (also involving fraudulent identity documents, for example to open accounts in bank branches, e.g.[B130][B139][B265][B327][B329]). 34 references.

5.2.2 Criminal business models

As presented in the overview of the online business model behind cybercrime from the UK National Cyber Security Centre *Cyber crime: understanding the online business model* [235], organised crime groups will either rely on own 'in-house' processes, outsource certain activities or sell data to other criminals (known as secondary fraud) to turn stolen data into profits. This section briefly discusses such business models from the 71 related references in the dataset (in Table 5.2).

To run their criminal business effectively and at scale, large organised crime groups have similar structures and requirements as legal enterprises, recruiting and employing employees with various skillsets (e.g. in [B103]) and in some cases running their criminal business as a nine-to-five operation [B161]. This is not an option for most smaller setups or individual attackers — certain specialist skills will need to be outsourced.

Many examples in this category refer to criminals providing products and services to other criminals, also called crime-as-a-service or secondary fraud [235]. These products and services may include stolen data, but also malware tools to enable others to commit crimes. These tools are often "competitively priced, with a rich feature list" and a "simple point and click interface" [B13], even including dedicated customer service and support. These "professional-grade banking trojans" designed to help steal login details for online bank accounts [B21] do not only offer high-grade technical support, but also customisation options [B109]. Other tools to launch large-scale DDoS attacks to bring systems down also exist, e.g. Titanium/Lizard Stresser in [B180]. Similar to organised crime groups focused on direct fraud, such secondary fraud providers may also show sophisticated structures with a number of employees, significant turnover and users, e.g. in [B156]. Smaller setups may sell compromised data such as personal information or credit card details directly on dark web forums [B202]; also in [B54][B148][B154][B183][B288]. Here, alternative payment services such as Bitcoin may be used for anonymity [B192].

Furthermore, many criminal business models will rely on additional infrastructure, such as suppliers and banks (e.g. Western Union or MoneyGram in [B159]) supporting their illegal business unwillingly (or willingly in [B91]). This criminal ecosystem also includes other services, such as professional money laundering providers [B187], money mules for extracting cash or criminals offering hosting services as well as other supporting service like fraudulent identity documents [B202].

5.2.3 Level of risk-acceptance in attackers

One of the attractions of cybercrime for criminals is the relatively low risk even for profitable and high volume attacks, inherently helped by the remote and anonymous nature of the internet (e.g. in [B83][B99]), but also low levels of protections and inefficient cybercrime policing (refer to Sections 5.3.5 and 5.3.6). And as cybercrime or cyber enabled crime offers a high potential financial yield at such a low risk to attackers, "there is no reason for criminal enterprises not to double their bets on international bank crimes" from a cost-benefit perspective [B92].

While cybercriminals will take precautions to reduce their risk, for example by attempting to delete their tracks [B85][B141][B178][B326], some decide to take measured risks, for example by marketing their criminal services on social media [B93]. Other individuals getting into cybercrime may be forced to accept a certain amount of risk due to a lack of alternatives — for example, young and educated programmers may not be able to easily access gainful and legal employment opportunities in certain geographic areas [B104]. In contrast, certain attacker types will engage in difficult and risky criminal operations — they may however also be better at hiding their tracks (e.g. in [B6]: Chinese hackers backed by the government). And cybercrime is not risk-free for all — one mistake may reveal the identity of a cybercriminal and lead to their arrest, for example "by accidentally connecting to the botnet directly from his home computer rather than the VPN" [B19]. Lastly, less-skilled individuals supporting cybercrime, especially when working on the inside of a target organisation, may lack the ability to hide their actions and hence face a far greater risk of being caught (e.g. in [B213]).

Codes (first level)	Sources	References
All in category code	227	1056
Characteristics of investigation	57	97
Charges	109	332
Sentences	66	237
Other consequences of attacks	52	72
Positive enablers	82	239
Hinderances and deterrers	32	79

Table 5.3: ***Coding overview for investigation and prosecution category code***

5.3 Investigation and prosecution

This section describes factors relating to the investigation and prosecution of cybercrimes against digital banking systems as identified in the dataset and shown in Table 5.3. In contrast to all other category codes covered so far, the contents in this category are not directly relevant to describing and profiling the characteristics and behaviours of digital banking attackers themselves. However, as these results can potentially be viewed as valuable in the context of criminal investigations and policing for cybercrime, the key insights are summarised in this section. Furthermore, it is assumed that understanding certain aspects of cybercrime investigation and prosecution may help to better explain some attacker behaviours.

5.3.1 Characteristics of investigation

Cybercrime investigations are generally presented as large scale, targeted and complex campaigns. To support this, they will often rely on collaboration between police forces, prosecution and the banking sector, at a national and international level. Examples include collaborative operational projects and task forces such as European money mule action project [B143], the FALCON taskforce [B174] or UK joint fraud taskforce [B144], but also dedicated and targeted operations, e.g. led by Europol [B189] or the NCA in the UK. An example for such an NCA-led campaign includes the targeting of an international crime network involving over 100 officers from across the UK, along with regional organised crime units, Immigration Enforcement as well as representatives from Moldovan and Romanian authorities in [B190]; with similar examples in [B182][B174]. While usually intelligence-led [B174][B214], such campaigns are also likely to rely on a number of physical searches and raids, e.g. in [B39][B54][B73][B189]. In these complex and sophisticated collaborations, a division of labour is often present: e.g. in [B210], a wide-reaching investigation involving Europol, UK and European authorities and the Royal Canadian Mounted Police is described, with the UK units responsible for executing local warrants.

Despite most investigations and campaigns showing high levels of structure, sophistication and collaboration, an element of coincidence may also support investigators: cybercrime suspects may be caught during routine checks, e.g. by border police at airports for undeclared items [B183] or when using false identity documents [B174][B177][B181]. Tip-offs seem to

play a small role here, with only one reference [B119] showing thieves mistrusting each other and one case of a cybercriminal being handed over to the police by their employer [B201] — vigilant co-workers may also help to discover cases of malicious insider involvement, e.g. in [B267].

5.3.2 Common charges for cybercrime

Cybercrimes may be classed under a variety of charges. From the analysed dataset, the following categories of charges can be identified for cybercrimes in the area of digital banking:

- Fraud, including conspiracy to defraud, steal or possession of articles for use in fraud (82 references in total identified in sample)
- Computer misuse and intrusion (48 references)
- Membership in a criminal organisation (10 references)
- Racketeering, including involvement in a racketeering enterprise or scheme (15 references)
- Other charges, e.g. possession of criminal materials (such as false identity documents), breaches of immigration law, drug related charges and any other criminal charges, e.g. failure to appear at court (42 references)
- Supporting crimes, e.g. identity theft and fraudulent identity documents, money laundering or non-computer theft (134 references)

5.3.3 Sentencing in cybercrime

Provided this list of charges, what sentences can cybercriminals then expect? Overall prison sentences seem to be the primary punishment for cybercriminals, although there is a significant variety in sentencing, including alternative or no sentencing at all. Using the example of the large-scale RBS WorldPay attack, the suspended sentence handed out is criticised as "too mild" in [B74], also pointing out the apparent differences in sentencing between Europe and the stricter laws and longer sentences applied in the US. This cannot be confirmed conclusively in the sample, although the longest sentences coded under 'prison sentence: long' are received by cybercriminals sentenced in the US (20 years jail term for a key crime gang member in [B25]). However, relatively long sentences have also been given to UK cybercriminals (8 years in [B200] or 11 years in [B181] for two fraud ringleaders).

Specifically, the following variations for the code 'sentence' can be found in the sample:

- Prison sentence (151 references in total identified in sample)
  - Long, duration over 5 years (43 references)
  - Medium, 2 to 5 years (59 references)
  - Short, under 2 years (48 references)
- Suspended prison sentence (28 references)

- Community service (12 references)
- Fine or repayment (18 references)
- No prosecution or sentence, for example due to health reasons or procedural errors (12 references)
- Sentencing for young offenders, for example juvenile warnings, suspended sentences or community services (6 references)
- Other sentences, for example deportation, a ban from using bank accounts or an order to attend rehabilitation facilities (10 references)

5.3.4 Other consequences of attacks

This short section describes any observed consequences of attacks outside of sentencing, for cybercriminals, but also for investigators and prosecutors as well as users. Firstly, there are the direct negative impacts of the attacks, like the cost and time to recover and restore adequate protection levels and might also include fixing exploited vulnerabilities. An example explaining this is the aftermath of an Anonymous attack faced by PayPal where "more than 100 workers [...] spent three weeks working on issues related to the attacks". They "also had to pay for more software and hardware to defend against similar attacks in the future", with the total cost estimated at £3.5 million [B10].

There are however also potential longer-term negative impacts: an organisation suffering from an attack may have to deal with reputational damage and may be going through the lengthy process of reclaiming funds where possible [B92][B123][B149][B160] [B211][B281][B309]. As a more positive effect, reported attacks and cybercrimes as well their investigation and related sentencing may help to raise general awareness of cybercrime risks [B152][B162] but also send a strong message to criminals [B13][B80][B189]; as discussed in Section 5.3.3: here, it is assumed that strict sentencing will serve as a deterrent.

5.3.5 Factors for effective investigation and prosecution: enablers and positive contributors

An interesting facet of the analysis results are the identified factors contributing towards (or hindering) effective cybercrime investigation and prosecution. Two categories of enablers and positive contributors can be made out in the sample: strategic, wide-ranging collaboration and effective, stringent and skilled law enforcement.

For the first category, the following relationships, collaborations and methods of cooperation are deemed as beneficial:

- *Cross-border collaboration between countries* — e.g. "the operation was part of a global effort, headed by the FBI, that involved nineteen different countries" [B142] or "law enforcement agencies and judicial bodies from Belgium, Denmark, Greece, the Netherlands, Romania, Spain and Portugal join forces in the first coordinated European action against money muling" [B143]. 35 references in total identified in sample.

- *Collaboration with industry partners* — e.g. industry-wide programmes in [B143][B144] [B148][B190][B208][B324] or between individual banks, e.g. in [B38][B149]. 44 references.
- *Collaboration with attackers or (former) criminals* — e.g. through a cooperation with investigators [B64] or plea with prosecutors [B288]. 21 references.
- *Collaboration with government and law enforcement agencies* — e.g. the NCA [B197] or regional organised crime units in the UK [B144], Europol [B152]: "mobile cyber forensic lab provided by Europol" or involvement of worldwide law enforcement agencies, e.g. Japan, Canada, the UK, Romania and 12 other countries in [B16]). 11 references.
- *Collaboration between multiple entities* — e.g. between law enforcement, financial sector and government agencies [B144] or [B105]: "Intel, Microsoft, security software companies F-Secure, Symantec, and Trend Micro; and Carnegie Mellon University also supported the operation". 10 references.
- *Collaboration with academia or external security experts* — e.g. in "the scale of the problem led the FBI to team up with European law enforcement agencies, the Georgia Tech Information Security Center and other security experts to track down the perpetrators" [B19]. 4 references.

Secondly, several elements to help effective law enforcement can be synthesised:

- *International law enforcement* — ideally, strict and consistent cybercrime legislation as well as a vigilant culture to cybercrime should be in place across any jurisdiction involved in cybercrime activities, e.g. in [B21][B80]][B151][B184]. 47 references.
- *Specialist institutions for cybercrime policing* — many references mention targeted, specialised institutions as key to successful cybercrime investigations and prosecutions, e.g. the Metropolitan Police central e-crime unit or the London regional fraud team in the UK [B151][B214] or Europol's European cybercrime centre and its joint cybercrime action taskforce [B152]. 34 references.
- *Building national capability* — in direct relation to the last aspect, empowered and highly skilled national institutions for policing and law enforcement seem to play a significant role when effectively dealing with cybercrime, e.g. in [B61][B146][B174][B189]. 13 references.
- *Other potential contributors* — e.g. monetary rewards for information leading to arrest or conviction of cybercriminals [B218][B223][B227], new effective cybercrime laws [B52][B73] or undercover agents [B98][B121][B291]. 18 references.

5.3.6 Factors for effective investigation and prosecution: hindrances and deterrers

In contrast to the last section, there are also a range of factors working against the effective investigation and prosecution of cybercrime. In this context, the following aspects should be considered:

- *Improper cultural attitude towards cybercrime* — a lax and 'nonchalant' cultural attitude to cybercrime in several jurisdictions [B39][B74][B109][B114][B288] and the often related inappropriate punishment [B46][B81][B99][B107] is seen to deter effective cybercrime prosecution. 21 references in total identified in sample.
- *Inadequate responses to cybercrime from banks* — banks and financial services institutions themselves may make cybercrime investigations and prosecution difficult by reporting breaches late [B40], not sharing information [B94] or even indirectly supporting criminal activities by accommodating money laundering activities [B103]. 13 references.
- *Unsuitable legal frameworks* — legal hurdles may also hinder cybercrime investigation and prosecution, e.g. a lack of reciprocal agreements between countries [B6], high corruption levels [B99][B104] and insufficient and antiquated cybercrime laws [B120]. 29 references.
- *Inefficient prosecution procedures* — while cybercriminals go to great lengths to avoid being caught and prosecuted [B33][B76][B145] and identifying individual attackers and the human behind an attack is inherently difficult [B52], there are also inefficiencies in prosecution, e.g. a lack of proactive intelligence gathering and sharing [B107][B275] or a perceived focus on prevention rather than prosecution [B81][B324]. 16 references.

5.4 Key findings and reflection

In this section, a presentation of key points arising from this chapter is made. This is followed by a reflection on current perceived limitations and an outlook on potential next steps and further research based on these results. The following 10 statements summarise the key findings on attack-related aspects and behaviours in attackers targeting digital banking systems from the grounded theory analysis of our sample. Although general in nature, it is hoped that these statements capture the central outcomes of the analysis undertaken. The following attack-related aspects and behaviours can then be described from the sample reviewed:

1. *Target distribution: national perspectives and casting the net wide* — where possible attackers seem to try and expand their attack campaigns to multiple countries, benefitting from the global and remote nature of cyberattacks. However, a significant number of domestic attacks within national borders can also be observed in the sample and many global attacks will also have certain local elements, e.g. language adaptation.
2. *Substantial losses and monetary damage* — the results seen in the sample confirm the large monetary damage and losses encountered, with most references recording losses through cybercrime incidents ranging between £1 million and £100 million, although significantly higher have also been observed. Several references also confirm the potential life changing effect cybercrime attacks may have on individual users. Both of these findings are in line with related literature.

3. *True cost of cybercrime difficult to quantify* — while many sources in the dataset quantify cybercrime losses in monetary terms, inclusion of damages beyond this type (e.g. reputational or cost for fixing exploitable vulnerabilities) are limited, highlighting the difficulty of defining the true cost of cybercrime to organisations and also economies.

4. *Banks and their ecosystem as targets* — while banks are naturally the focus of digital banking attacks, attackers will consider and research the complete ecosystem including external third-party suppliers, which may display lower protection levels than the banking organisation itself.

5. *Target attractiveness and opportunity* — generally, cybercriminals seem attracted by opportunities to commit a crime at a relatively low risk, but ideally with high profits (cost-benefit ratio). Examples for this phenomenon include attacks on primarily developed economies, cash-rich countries as well as known vulnerabilities provoking attacks.

6. *Controversy around liability* — although only referenced in a small number of sources, the question around liability for digital banking fraud losses between banks, third-party suppliers and customers seems relatively open at this point in time. While recent strengthening of customer protection shifts the liability towards banks, increasing fraud losses add additional pressure to banks to pass some of this liability on.

7. *Evolving threat landscape and changing attack vectors* — new threat vectors specifically relevant to digital banking seem to have emerged in recent years, adding to the attack vectors and means observed in the sample. This underlines the speed of change in this area, with new attack patterns and vectors being developed all the time by attackers, also to keep up with the ongoing defensive efforts on the side of organisations.

8. *Supporting non-technical means* — crimes and attacks against digital banking heavily rely on supporting means such as money laundering, cash extraction and identity fraud. Money mules for example will help to move money through various legitimate accounts rapidly, disguising its criminal origin before withdrawing the funds in cash, but also increasingly through other means like bitcoin schemes, e.g. in Krebs [242].

9. *Sophisticated business model behind cybercrime* — often, cybercrimes are not committed in isolation, but are part of a larger ecosystem, with sophisticated, large organised crime groups at the centre of these business models of crime.

10. *Enablers of effective investigation and prosecution* — successful cybercrime investigations and prosecution processes mentioned in our sample usually contain elements of international cooperation and collaboration across a wide number of institutions (including industry partners). Advanced and specific skills for cybercrime investigations also seem beneficial, with special cybercrime units supporting many investigations. Furthermore, strict, proactive and efficient law enforcement procedures are seen as necessary to ensure effective prosecution.

Considering these overall results and key findings presented in the last section, several limitations and potential for further research can be identified.

- *Current and upcoming threats* — as mentioned in Section 3.4, recent attack vectors

against digital banking systems are unlikely to be adequately covered in the sources included in the analysed dataset (due to the date range of the sources). It is therefore of crucial importance that further sources containing such current data are reviewed and added on an ongoing basis. This will also support gaining an understanding of risk profiles of innovation in the area of banking (e.g. blockchain or cryptocurrencies).

- *Legal aspects and questions around liability* — the legal setup around cybercrime, with largely anonymous attackers and remote attacks paired with often ineffective legal frameworks across various jurisdictions, can be considered as difficult. While this observed complexity is not fully accounted for in this research, further research efforts in this area are outside the scope of this thesis.
- *Elaboration on cybercrime business models* — large groups, sophisticated group structures and secondary fraud schemes are referenced numerous times throughout the sample, corroborating and aligning with presentations in literature like the NCSC study on business models underlying cybercrime [235]. As this aspect is likely to carry significant weight in the context of digital banking fraud, the limited treatment in this study leaves room for further research focussing on this topic specifically in the future.
- *Decision-making for selection of targets* — within the reviewed sources, the reasoning applied when choosing targets by attackers is limited to two logical explanations: target attractiveness and the level of opportunity presenting itself. However, this gap can potentially be filled by reviewing aspects of attacker motivation (profit and non-financial) as discussed in Sections 4.1.8 and 4.1.9.
- *Effects of cybercrime attacks on individual users* — sources referring to financial losses and damage encountered by individual users are limited in the reviewed sample, making a dedicated enquiry into the victimology of digital banking fraud difficult in the context of this research. Future research efforts are likely to require a different methodology and source dataset.

There are several opportunities for further meta-analysis of this data and the key insights stemming from the analysis in this chapter and previously Chapter 4. The results from this chapter can also be viewed to support the definition of distinct attacker types applicable to digital banking in Chapter 6, specifically modus operandi aspects. But insights from this chapter also directly support the work carried out in Chapter 7, where many findings and references are used directly to build and illustrate the attacker personas. In particular the supplementary narrative scenarios shown in Appendix A benefit from the gained knowledge around business models, reasons for selecting targets or encounters between cybercriminals and the law. The emerging categories in this chapter are also briefly reflected on and considered for their overall usefulness in the context of security practice in Chapter 8.

Part III

Meta-Analysis

Despite these findings, which overall indicate a disheartening picture of state-of-the-art thinking on threat actor typologies, a certain common basis for building a cyber attacker typology emerges.

— M. de Bruijne, M. van Eeten, C. Hernàndez Gañàn, W. Pieters, 2017 [26] p.25

6

A New Attacker Typology for Digital Banking

This chapter elaborates on the analysis in Part II by identifying clusters of attackers from the data sample. It aims to provide a grounded and structured representation of attacker types specific to digital banking, in close alignment to the existing research field of attacker categorisations in the form of taxonomies or typologies. As a result, seven distinct attacker types are proposed here. Furthermore, a compact critical excursus into circumplex visualisations as a commonly used vehicle in previous research is provided, as well as a presentation of validation efforts undertaken for our typology to date.

Systematic attacker categorisations in the shape of taxonomies or typologies have been at the centre of past research as discussed in Section 2.3, with their aim of representing variations within attacker communities, expressed in differences in technical skills, motives or level of damage caused. This chapter documents the results of building such a categorisation framework specifically for digital banking attackers, using the research procedures set out in Section 3.5.2. While this exercise can be viewed as a sequential progression and meta-analytical step from the last two chapters documenting characteristics and behaviours of such attackers, it also aims to address several potential limitations found in earlier works (including the frequently cited standard work on hacker taxonomies by Rogers [46][23]).

As outlined in Sections 2.3 and 3.5.2, specifically in the critical analysis of threat actor typologies by De Bruijne et al. in [26], previous research efforts have often shown a lack (or at least limitation) of transparency and completeness in regard to their methodology and used data sources. In response to this starting point from prior research, and incorporating the results from Chapters 4 and 5, exact research procedures have been devised in Section 3.5.2 to create a dedicated, new attacker categorisation for digital banking attackers based on real-life data from secondary sources. These procedures have made note of previous methods including naming conventions (mainly reflecting on the distinction between the terms 'typology' and 'taxonomy', see p.31), described the full typology building process using NVivo as software support and paper-based affinity diagramming as well as noted the intended methods of validation and feedback implementation.

Additionally, the intention was to supply a 'circumplex model' for the here presented typology, to align and enable comparison of our results with previous works in the research area using these visualisations such as Rogers [23], Hald & Pedersen [24] or later Seebruck [25]. However, as circumplexes have been referred to relatively uncritically and in a different sense to their traditional usage (as a statistical model and data analysis tool) in this context, a further enquiry seems warranted at this point. A dedicated section (excursus) briefly outlining the origin of circumplex models, also analysing their potential problems and advantages for attacker categorisation, is therefore included here (in Section 6.3) before producing an example circumplex specific to digital banking (see Figure 6.9).

Based on the background provided in Section 2.3 and adhering to the methodological procedures in Section 3.5.2, this chapter first and foremost supplies a full overview of the results from the categorisation building exercise undertaken and is structured as follows. Firstly, seven distinct attacker types as found in the analysed attacker population are shown using a table format in Tables 6.1 to 6.7, based on the categorisation criteria as defined in Section 3.5.2 and Table 3.9. Additionally, visual representations of direct quotes from the source materials specific to each attacker type have been created in Figures 6.1 to 6.7, to help maintain a continuous and close relationship with the original dataset throughout the research project. Following the order of the research procedures, an evaluation using heuristics specific to typologies or taxonomies (as adapted from De Bruijne et al. in [26]) is completed next, followed by an overview on feedback received via peer review for the initial iteration of this work — subsequent actions taken to progress this work to its current state from these two feedback loops are also listed here. Next, a compact excursus on circumplex visualisations is attempted, including a new circumplex representation specific to the attacker landscape analysed in this thesis, but also a critical assessment of their value when building or using typologies or taxonomies. Lastly, this chapter is rounded off by a brief summary and reflection, also providing a transition into the later chapters on attacker personas and attacker-centric security.

6.1 Results

Seven distinct groups of attackers have been identified using the research procedures as set out in Section 3.5.2 and based on the sample used within this thesis (data sources as listed in Section 3.4 and shown in Appendix B), forming an attacker typology specific to digital banking (with the specific and unique nature of this domain as a case example outlined in Section 2.5).

The following pages provide seven overview tables showing the different attacker type categories with their relevant details. As prepositioned in the research procedures in Section 3.5.2, several gaps in these tables remain or findings need to be viewed as tentative. Where this is the case, one asterisk (*) is used to signifiy a weak evidence base (low number of references from the data) and two asterisks (**) are used where an assumption was made — this is also commented on directly within the overview table where necessary. Where data sources are directly referenced, the already known format [B123] from the last chapters is used, referring to the list of individual source materials included in Appendix B.

As indicated in the introduction, each of these overview tables is also accompanied by a visual representation of original quotes from the data sample. These data fragments have been selected largely at random by the researcher from all the codes relevant to the attacker type category with the aim to represent all coded references, although a level of editing is present to avoid for example overly similar quotes. Following the same principle as in the overview tables, the origin of these excerpts is made clear with a reference to Appendix B.

6.1.1 System challengers category

Group	**System challengers**
Subgroups	System testers, hackers looking for fun or challenge
Labels	White hat or ethical hackers*, thrill seekers or glory hunters, young or novice hackers
Motives	Fun of hacking, bragging rights, challenge to break into system, exposing vulnerabilities (responsible disclosure**)
Criminal intent	Low to moderate
Resources	Range of skills and funds, can be limited
Activities	System intrusion, penetration testing, publication of vulnerabilities
Level of danger posed	Relatively low, but varies across the group and can be seen as an entry into serious criminality for some
Type of risk posed	Often reputational risk, may however also be of financial or operational nature
Other notes or comments	Very heterogeneous group united by desire to overcome system's defence — in our sample, the number of white hat/ethical hackers seems low with only limited evidence, e.g. in [B70]. Responsible disclosure cases were not present in the sample, but this option, where (non-malicious) attackers would notify banks about identified vulnerabilities to provide them with the opportunity to fix them before going public, is made available by a number of banks, e.g. The Royal Bank of Scotland in the UK [361].

Table 6.1: ***Attacker profile for system challengers category***

“Do we really believe that a lone hacker gets into a [certificate authority], can generate any cert he wants...and goes after login.live.com instead of paypal.com?” [B29]

“Then I wrote and sent a formal report to all the CEO of banks in Iran but none of them replied to me.” [B70]

The hackers claim they hack for the “lulz”–for fun–and also to point out security vulnerabilities in networked systems, according to statements attributed to the group on Twitter and posted to the LulzSec web site. [B55]

He reportedly told them he was motivated not by greed, but rather a love of computers and an ambition to be a software developer. [B18]

“Around one year ago I found a critical bug in the system” [B70]

He was only 16 when he started to do this and it was his immaturity and naivety which led him to commit these offences [B157]

A computer hacker who ruined a man's internet firm 'for a game' and was caught with thousands of stolen bank account details [B155]

The group announced on June 15 that it was able to steal AmeriCash's customer data because the company had left a confidential page unsecured on one of its servers. [B320]

"I haven't broken any laws," he said. "I have nothing to worry about." [B55]

“Not only was this page unsecured, it was actually referenced in their robots.txt file (bad, bad move, guys)." [B320]

Figure 6.1: ***Data excerpts for system challengers category***

6.1.2 Supporters category

Group	**Supporters**
Subgroups	Money mules, non-technical support functions
Labels	Non-technical support functions: mules, cash collectors, business functions such as recruitment, marketing or customer service
Motives	Financial gain, 'making ends meet'
Criminal intent	Moderate to high (in some cases unwittingly)
Resources	Limited technical skill levels and funding
Activities	Supporting a larger group or system through all stages of money laundering and other business support functions
Level of danger posed	Low on their own, but part of a group or system
Type of risk posed	Usually financial risk, although operational and reputational risk may be indirectly posed
Other notes or comments	Supporters are not technically attackers themselves, but support others to commit their crimes. These functions are relatively well evidenced in the sample, with over 100 related references present.

Table 6.2: ***Attacker profile for supporters category***

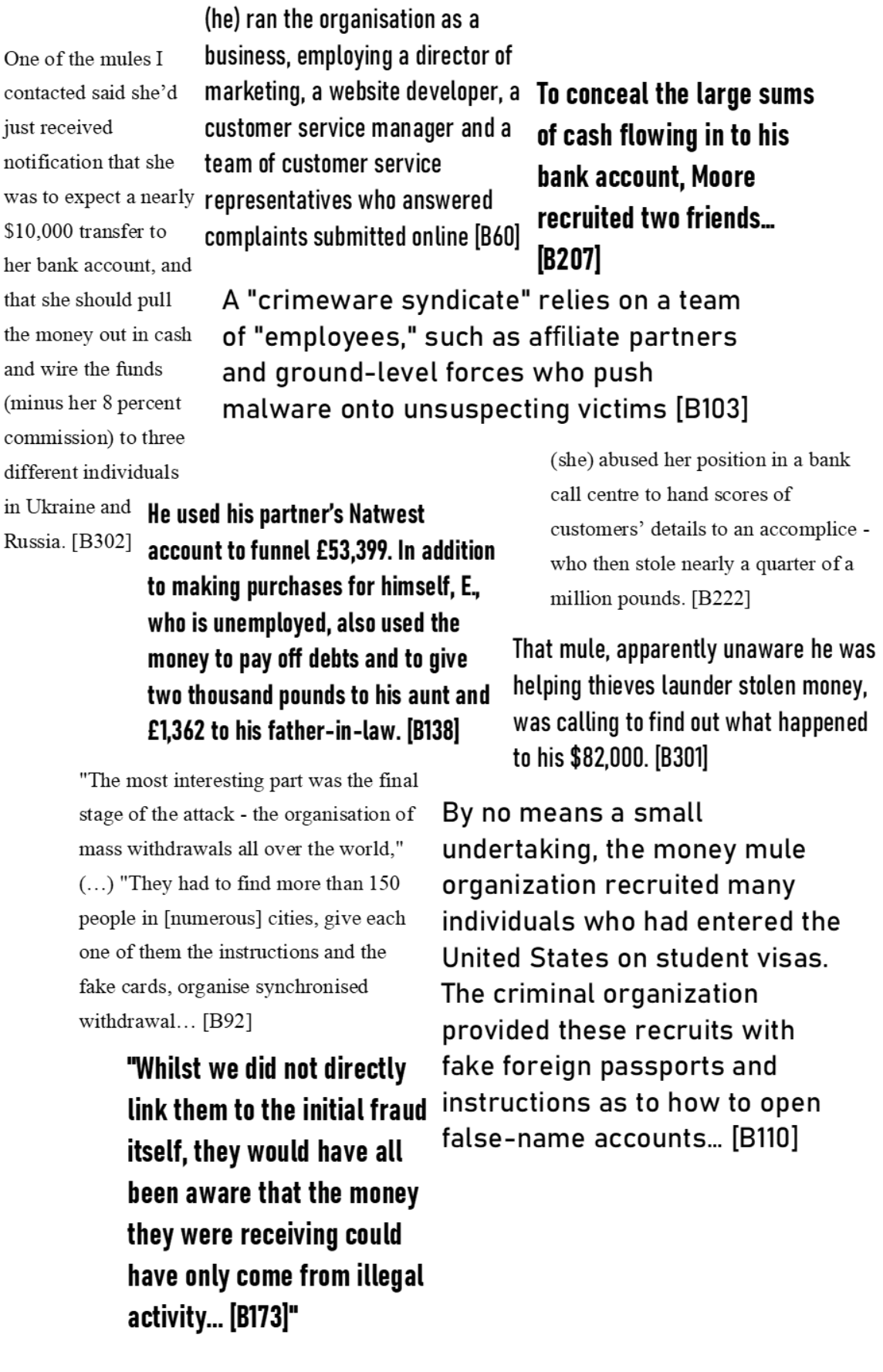


Figure 6.2: ***Data excerpts for supporters category***

6.1.3 Insiders category

Group	**Insiders**
Labels	Banking employees, third party supplier employees
Motives	Financial gain, retaliation*
Criminal intent	Moderate to high
Resources	Range of skills and funds, enabled through insider knowledge and capabilities including elevated access rights
Activities	Usage of insider knowledge to extract money directly (or enable others), IT sabotage/system destruction*, industrial espionage*
Level of danger posed	High, significant levels of damage possible
Type of risk posed	Often financial, but also significant potential for operational (IT sabotage*) and potentially reputational risk
Other notes or comments	Highlighted in the extensive works on insider threats from Carnegie Mellon University [362], financially motivated insider data theft is committed by individuals with all levels of technical expertise, whereas sabotage attacks affecting operations and reputation are more likely to have tech savvy individuals behind them — this is partially supported by case examples in the examined dataset: e.g. [B160][B165][B291][B306] describe banking employees at all hierarchy levels and with varying skillsets abusing their trusted position, while [B243] describes targeted DDoS attacks against financial institutions in the US by a highly skilled groups of attackers. Cases of sabotage/system destruction or industrial espionage are however limited in our sample, e.g. in [B108][B268].

Table 6.3: ***Attacker profile for insiders category***

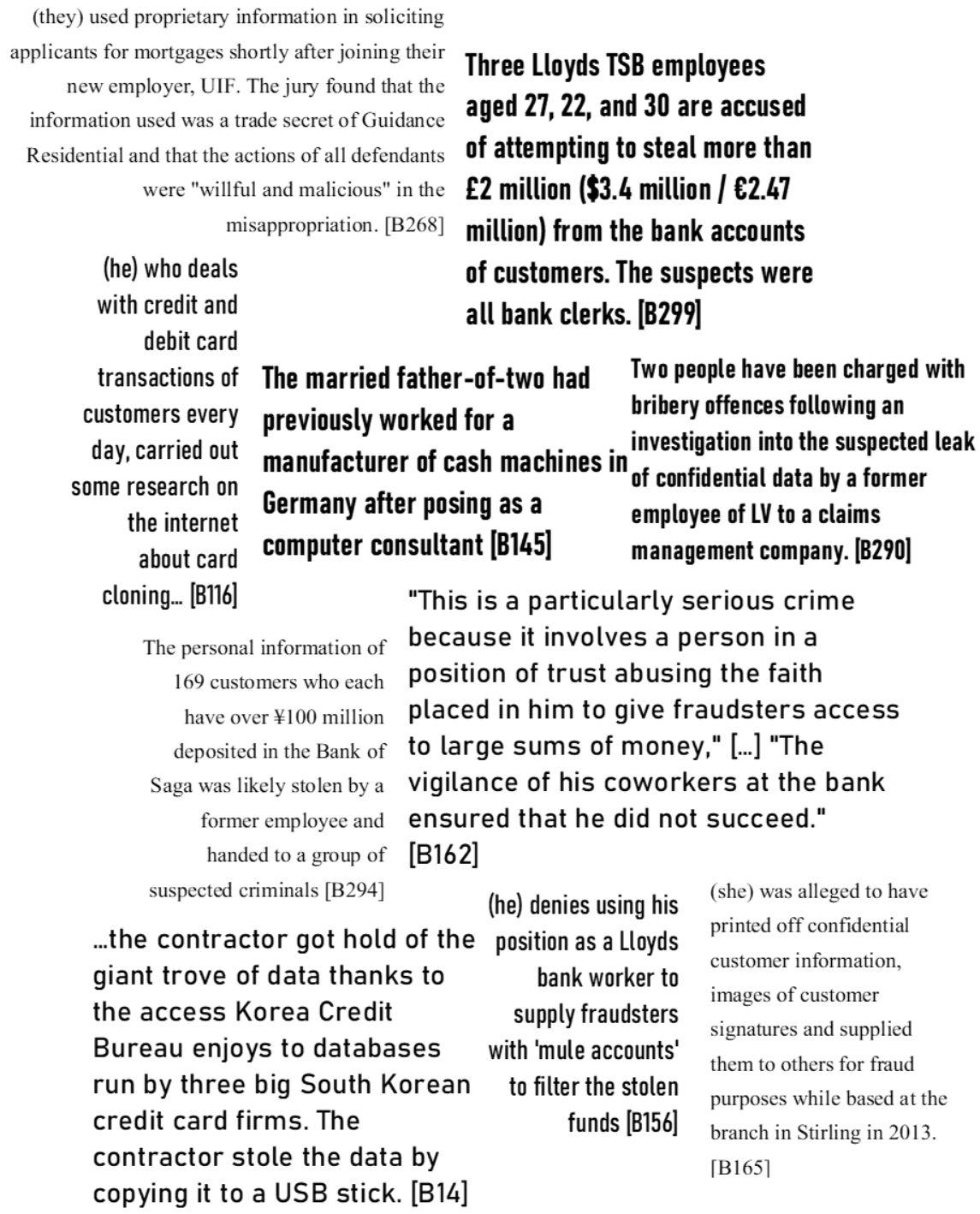


Figure 6.3: ***Data excerpts for insiders category***

6.1.4 Ideologists category

Group	**Ideologists**
Labels	Hacktivists, online activists or cyber terrorists
Motives	Cause, ideology, in rare cases also status and ego (secondary motives such as financial gains may be present*)
Criminal intent	Moderate to high
Resources	Moderate to high skill levels and funding
Activities	Social or political background to attacks
Level of danger posed	High, significant levels of damage and destruction intended
Type of risk posed	Reputational risk and linked operational risk, financial risk as a secondary motive*
Other notes or comments	Ideologists are usually motivated by cause and ideology, but examples of attackers being motivated by selfish reasons such as financial gain or simply to engage in petty vandalism can be found, e.g. in [B55][B123][B320].

Table 6.4: ***Attacker profile for ideologists category***

Despite an advance warning by attackers, all of the targeted banks' websites still suffered disruptions. [B108]

PayPal and Mastercard stopped allowing users to donate to the Wikileaks website and as a result the money transfer organisations became a target for the Anonymous group who plotted revenge in a ploy nicknamed 'Operation Payback'. [B218]

"Operation Anti-Sec might read like something from a cyberpunk novel but in reality it is being used by far too many to lay a thin veneer of altruism over something entirely selfish... [B123]

Anonymous claims it filched the list from computers belonging to the Federal Reserve. Just as the Super Bowl was ending, Anonymous declared on Twitter, "Now we have your attention America: Anonymous's Superbowl Commercial 4k banker dox via the FED." [B310]

Hackers left a deface page along with a note on the website, but the reason for targeting MasterCard website wasn't mentioned anywhere. [B286]

A hacktivist group known as the European Cyber Army said Jan. 28 that it had waged targeted distributed-denial-of-service attacks against Bank of America and JPMorgan Chase. [B260]

"I think the hackers we really need to worry about are those that trusted no-one and sought no glory in the first place." [B134]

The official websites of two Turkmenistan state-owned commercial banks have been hacked and defaced by Dr.Sha6h, the Syrian hacktivists who has defaced government websites from all over the world in an effort to raise awareness of the situation in Syria. [B300]

A system administrator for an unnamed company was caught defacing his own firm's website to hide the theft of company data, which he planned to sell and then retire to a seaside town abroad. […] When he came back to work the next day, he used his admin panel credentials to deface one of the company's websites with a message from a hacktivist group accusing the firm of globalization. [B267]

Figure 6.4: ***Data excerpts for ideologists category***

6.1.5 Officials category

Group	**Officials**
Labels	Nation states, sovereign countries, governments or their agencies, military functions*
Motives	Cause, ideology, cyber warfare*
Criminal intent	High**
Resources	Very high skill levels and funding**
Activities	Espionage, counterespionage, information monitoring and destructive attacks, cyber warfare*
Level of danger posed	High, although limited evidence and confirmed cases to date*
Type of risk posed	Operational risk as a main focus with reputational and financial risk directly linked**
Other notes or comments	Not much is known about this group and references in the data sample are sparse, e.g. in [B6] or [B79], where nation state involvement in attacks affecting digital banking services is indicated, but no further detail on for example skill levels or activities are included (most likely as they are unknown). This attacker group is therefore marked as tentative, with several aspects not supported directly in the sample. It is important to realise that this does not necessarily mean that such attacker groups and their attacks are not relevant to financial institutions, but more likely that they haven't found entry into the analysed sample — this might be due to these attackers being able to stay under the radar and therefore not being reported on widely potentially.

Table 6.5: ***Attacker profile for officials category***

U.S. government officials have been reluctant to tie the attacks directly back to the Chinese government, but analysts and officials quietly say they have tracked enough intrusions to specific locations to be confident they are linked to Beijing — either the government or the military. They add that they can sometimes glean who benefited from a particular stolen technology. [B6]

(...) size and sophistication of Flame suggested it was not the work of independent cybercriminals, and more likely to be government-backed. [B79]

"His ramblings certainly show his support for Mahmoud Ahmadinejad and the current Iranian regime, but there are no conclusive ties to his government." [B29]

Each individual was a leader, contractor, associate, hacker for hire, or affiliate of the Mabna Institute, a private government contractor based in the Islamic Republic of Iran that performed this work for the Iranian government, at the behest of the Islamic Revolutionary Guard Corps. [B242]

Each defendant was a manager or employee of ITSecTeam or Mersad, private security computer companies based in the Islamic Republic of Iran that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps. [B243]

"The geography of the targets and also the complexity of the threat leaves no doubt about it being a nation-state that sponsored the research that went into it" [B79]

As few as 12 different Chinese groups, largely backed or directed by the government there, commit the bulk of the China-based cyberattacks stealing critical data from U.S. companies and government agencies, according to U.S. cybersecurity analysts and experts. [B6]

"They have been going after everyone-financial services, Wall Street," a senior defense official, speaking anonymously, told The Wall Street Journal. "Is there a cyberwar going on? It depends on how you define war." [B108]

Figure 6.5: ***Data excerpts for officials category***

6.1.6 Professionals I: groups and gangs category

Group	**Professionals I: groups and gangs**
Labels	Sophisticated large criminal groups or gangs and organised online crime syndicates with members often professionally recruited (e.g. in [B63] or [B101])
Motives	Financial gain
Criminal intent	High
Resources	High skill levels and funding: broad range of skills and resources available through group setup
Activities	Phishing, ransomware, trojans and malware attacks as well as system intrusion at large scale, physical attacks e.g. against cash machines also possible. May also offer their services through criminal-to-criminal franchise models.
Level of danger posed	High, significant levels of damage
Type of risk posed	Financial, operational and reputational risk directly linked
Other notes or comments	Primary/key category for digital banking attackers. These attackers should be viewed as highly professional criminals. This attacker group characterisation seems well supported in the sample, with over 200 references supporting activities and modus operandi aspects and a further 200 references on roles and functions in attacker groups.

Table 6.6: ***Attacker profile for professionals I: large groups and gangs category***

The head of a fraud ring has been sentenced to 11 years in prison for his part in a £113m scam […] he was the "leader and prime mover" and made almost all the calls, the court heard, making sure that they appeared to be coming from a location that would not arise suspicion. [B163]

VK, ST, OC and a fourth man, identified only as "Hacker 3," pooled their talents, and with the help of a worldwide network of "cashers" in more than 280 cities, they were able to walk away with $9 million of RBS WorldPay's money. [B326]

The Met's Police Central E-Crime Unit (PCeU) says K1 ran the operation from the Ukraine and was responsible for obtaining and allocating accounts to be attacked. K2 was K1's right hand man in the UK, organising the establishment and operation of recipient accounts. [B53]

One of the ringleaders (...) was jailed for eight years last month for organising the plot targeting customers of Barclays, First Direct and Co-Op. [B209]

The leader of a global cybercrime syndicate offered his associates a Ferrari for the hacker who came up with the best scam (...) formed the basis of a bizarre "employee of the month" competition for the organised crime gang. [B99]

Two years ago, police arrested five Ukrainians who were part of a 60-person group that used hosts in Britain to steal $70 million from US businesses. [B97]

The US Attorney for the Southern District of New York and the Manhattan D.A. charged 37 people Thursday, most of them Russian nationals, with stealing more than $3 million from small business and government accounts in the U.S. Another 19 suspects were arrested in London, and 11 were charged in the theft of $9.5 million from British banks. [B2]

Police in 16 countries across the United States, western Europe and in Chile have seized cash, firearms and drugs and arrested 80 people suspected of peddling virus software believed to have infected hundreds of thousands of computers, according to European legal authorities. [B60]

Fifty-seven people have been arrested in 25 separate operations, which relate to a range of cyber criminality... [B188]

(he described him) as being part of a "small cabal of leaders" and the network administrator for the group. [B10]

Figure 6.6: ***Data excerpts for professionals I: large groups and gangs category***

6.1.7 Professionals II: small groups and individuals category

Group	**Professionals II: small groups and individuals**
Labels	Lone hackers and individual attackers, small criminal groups and gangs (can be relatives or friends rather than recruited, e.g. in [B54] or [B302])
Motives	Financial gain
Criminal intent	High
Resources	Moderate to high skill levels and funding
Activities	Phishing, ransomware, trojans and malware attacks as well as system intrusion, physical attacks. Similar to professionals I, but usually at smaller scale.
Level of danger posed	Medium to high
Type of risk posed	Financial, operational and reputational risk directly linked
Other notes or comments	Primary/key category for digital banking attackers — small to medium group size including lone attackers based on approximately 100 references in the sample. Again, these attackers should be viewed as professional criminals.

Table 6.7: ***Attacker profile for professionals II: small groups and individuals category***

He is one of eight men, aged between 24 and 47, arrested on suspicion of being in a gang that stole the money in a Trojan Horse-style plot at a branch of Barclays. [B100]

Iserdo was arrested alongside with two other suspects in Slovenia as part of a joint FBI-Slovenian investigation that has since focused on the 23-year-old. [B19]

An alleged Algerian computer hacker wanted by the FBI on suspicion of stealing millions of dollars from US banks to fund a life of luxury has been arrested in Bangkok, Thai police say. The FBI have been tracking 24-year-old Hamza Bendelladj, a computer science graduate, for three years. [B9]

Two men have been charged with the suspected theft of £1m from two UK banks by the Metropolitan Police's new Cyber Crime Unit. [B37]

Police said they found computer scripts used to run the fake banking websites when the men were arrested in August 2010 at locations in London and Navan, County Meath, Ireland. It's believed the three obtained details on more than 900 bank accounts and 10,000 credit cards. [B72]

(...) the small crew of hackers had a distinct division of labor, operated with skill and efficiency and left one of the world's larger banks holding the bag... [B326]

"I'm not a group of hackers, I'm single hacker with experience of 1,000 hackers" [B29]

A Russian programmer accused of being the mastermind behind one of the most commonly used bank account hacking kits has pleaded guilty to a related charge in the US. [B24]

(he) then gloated about the crime he committed to colleague T, who became part of his credit card data theft activities, among others, as revealed by further inquiries of PCeU. The two allegedly targeted online casinos/ betting companies as well as other Web hosting businesses. [B41]

Three men have been jailed after defrauding elderly bank customers of more than £390,000 and laundering the cash through multiple fake accounts. [B189]

Figure 6.7: ***Data excerpts for professionals II: small groups and individuals category***

6.2 Validation efforts

Validation efforts for the presented typology in this work are made up of two components as indicated in the research procedures section earlier (Section 3.5.2): firstly, feedback from academic peers was used to improve on the initial iteration of typology (as published in Moeckel in 2019 [275]). Secondly, this initial typology has been compared to a number of heuristic criteria formally defining a 'good' typology or taxonomy (based on quality indicators as set out by De Bruijne et al. [26] p.14). From these activities and their results, a number of changes have been made to help build the current, here presented typology iteration as summarised in the last part of this section.

6.2.1 Peer review feedback and resulting amendments

For the peer review of this typology, three sets of comments were used: two sets of reviewer comments from conference submissions and direct feedback from the UK PhD examination process. The venues submitted to were the First Workshop on Attackers and Cyber-Crime Operations (WACCO) at the IEEE European Symposium on Security and Privacy 2019 in Stockholm (weak reject) and the First International Workshop on Information Security Methodology and Replication Studies (IWSMR) at the 14th International Conference on Availability, Reliability and Security (ARES 2019) in Canterbury (accepted & published as [275]). The feedback obtained throughout the PhD examination process was provided by two senior academics working in the area of information security. As an excerpt of the extensive feedback provided[50], Table 6.8 lists the highlighted aspects in direct relation to the typology as well as actions taken to address these comments.

6.2.2 Heuristic review

The structure of the typology is also evaluated in a second step, based on a list of formal criteria for evaluating the quality of a taxonomy/typology as identified from literature in De Bruijne et al. [26]. Built from general (not information security or attacker specific) literature on classifications and their validation such as in Bailey [142], this list is seen to help provide further confidence in our typology, but also yield recommendations for improvements. The following lists the eight abbreviated evaluation criteria adapted from [26] p.14/15 and a brief assessment on how these are currently met in our typology.

1. *Exhaustive* — all potential attackers should be classified. While this criterion is difficult to meet without any restrictions as new and unknown attacker types may always present themselves over time (see also Criteria 7 and 8), the current typology builds on data

[50]It is worth noting that only a limited number of feedback items have been included here, mainly because they were not directly relevant to the actual typology itself, but e.g. its presentation in the overall paper or thesis or related to materials that were ultimately not included in the paper or thesis. The individual feedback items as shown in the table have furthermore been shortened and rephrased where required to make them as accessible as possible to the reader.

from a relative large dataset of real-world digital banking cybercrime cases, representing a varied population of attacker types for this case example.

2. *Mutually exclusive* — all potential attackers should fit into just one class. This criterion was not satisfactorily met in the original, initial iteration with eight attacker types as presented in Moeckel [275]: the attacker type class 'toolkit users' showed continuous overlaps with other categories, i.e. toolkit users would also be part of small or larger criminal groups or insiders — it was therefore decided to remove this group in the current iteration (see also Section 6.2.3).

3. *Relevant* — the classification method should facilitate consistent replication based on available information and lead to meaningful classification. The research procedures in Section 3.5.2 should enable replication using a similar dataset containing cybercrime cases (an exact replication from the original dataset used in this work would also be possible, refer to Appendix B).

4. *Pragmatic* — the typology must contain a manageable number of classes/attacker types that can be clearly distinguished, requiring observable heterogeneity between them, but also meaning a relatively high level of abstraction overall. The number of attacker type classes in our typology is limited (7), all showing relative levels of heterogeneity between each other (see also Criterion 2). Also remarked on in De Bruijne et al. [26], typology quality criteria may be conflicting in this context, owed to the balancing act between creating a compact and abstract, yet complete and detail-rich, typology (as required under Criterion 1).

5. *Efficient* — the classification method must enable efficient classification efforts. The research procedures in Section 3.5.2 should enable a streamlined classification process — however, any grounded and data-driven categorisation will require some effort through immersion into the source dataset and data analysis.

6. *Transparent* — the classification method should be based on a defined list of descriptive dimensions, accessible and clearly documented. The research procedures in Section 3.5.2 present the methodology used in full, including the reasoning behind the dimensions used.

7. *Dynamic* — the classification method should enable continuous updates to the typology to accommodate new available data. As stated throughout this chapter, the typology building exercise presented in this work is viewed as an iterative process — to accommodate new data in the typology, the research procedures as outlined in Section 3.5.2 would need to be repeated again and include any new materials.

8. *Iterative* — new attacker types can be added as a result of Criterion 7. In direct relation to the last point and as evidenced in the response to Criterion 2, attacker type classes can be added or removed in any new iteration of the typology.

Feedback/comment item	**Analysis/action item**
Usefulness/motivation: establish academic and/or practical value behind attacker categorisations and how they relate to risk models or threat modelling methodologies	To support this work, a new section assessing the potential and practical value of attacker categorisations, has been included in Chapter 2 of this thesis (Section 2.3.2).
Application to digital banking: highlight specific nature and features of the domain in comparison to other contexts	In addition to the above, a note on digital banking as a domain has now been added to guide the reader (Section 2.5).
Link to data: connection to the underlying dataset should be established, also surfacing details from the analysed materials.	Further references to the original dataset have been included directly in the attacker type overviews and visual representations of data fragments for each attacker type added (Figures 6.1 to 6.7).
Content dimensions across typology: is sufficient data available for every dimension and every attacker type from the analysed dataset? And are all dimensions relevant and required, e.g. criminal motivation when skill levels and equipment are already defined?	Where evidence in the data is limited or assumptions have been made, this has now been explicitly marked and commented on (asterisk usage). At this point, all dimensions are included for information purposes, but categories could be removed if they remain unused in practice for future iterations.
Assigned weightings across typology: where possible, assign a relative importance or impact to the attacker types	A note has been made within the attacker type overviews to indicate the most relevant categories based on the number of references within the sample.
Nature of categories within the typology: are the attacker types mutually exclusive and collectively exhaustive?	This suggests a formal examination of the typology structure — while this has not been completed in related works such as [23][24] or [25], a proposed approach is suggested in this section.
Circumplex models: critical analysis and reasoning behind their inclusion required	A dedicated excursus on circumplex models has been included in this iteration in Section 6.3, reflecting on their origin and usefulness as well as providing an example circumplex for our typology.
Validation: how can the new typology be tested/confidence be instilled?	Evaluation efforts have now been included in this section, with further validation efforts envisioned to help build future iterations.

Table 6.8: ***Consolidated feedback and action items for initial iteration of attacker typology***

6.2.3 From initial iteration to current typology and beyond

A number of changes to the initial iteration of this typology (published and available as [275]) have been made following the described evaluation steps (Table 6.8) to arrive at the current state as presented in this thesis.

- The most significant change was certainly the reduction from eight to seven attacker types, removing the 'toolkit user' class following the violation of the 'mutually exclusiveness' principle required for a well-structured typology. For transparency, the overview table of this removed category is shown in Table 6.9.
- Data from the original dataset this typology builds on has been surfaced better: via direct references and the data fragments displayed in Figures 6.1 to 6.7. Furthermore, where the level of confidence in findings is limited due to only very few supporting data sources, this has now been marked (as * or ** in Tables 6.1 to 6.7). A note on the weight of an attacker type category has been made where possible, based on the amount of supporting references and occurrences for these types of attackers in the sample.

Beyond this current state of the typology, further iterations should be expected to develop and improve the typology based on new developments and trends influencing the attacker landscape, but also from feedback following further evaluation efforts. Viable options here could include replication exercises using new source datasets, but also further input from industry subject matter experts or academic peers — potential future research directions are indicated in Section 6.4.3 of this chapter.

Group	**Toolkit users**
Labels	Users of attack toolkits (also called crime-in-a-box, exploit or crimeware kits), clients of criminal-to-criminal services (also named crimeware-as-a-service)
Motives	Financial gain, 'making ends meet'
Criminal intent	High
Resources	Limited skills and funds (relying on toolkits), experienced attackers may use them for convenience/scalability
Activities	Phishing, ransomware, trojans and malware attacks through usage of toolkits and services available through criminal-to-criminal franchises.
Level of danger posed	Medium to high
Type of risk posed	Financial risk, operational and reputational risk directly linked

Table 6.9: ***Attacker profile for toolkit users category (removed)***

6.3 Excursus: circumplex visualisations

As indicated in the introduction and background section of this work, the usage of circumplex models as a visualisation tool can be observed throughout key works in the area of attacker typologies and taxonomies such as Rogers in 2006 [23], Hald & Pedersen in 2012 [24] and lastly Seebruck in 2015 [25] (compare to Figure 6.8; also mentioned in De Bruijne [26] p.23). In this compact excursus, the origin of these models is briefly discussed, including their traditional usages, how they have found entry into the area of typologies/taxonomies and what their realistic value is when used as part of attacker categorisations. To help illustrate the last point specifically, a customised circumplex representation for the case of digital banking, based on our typology, is created in Figure 6.9 (p.166).

Circumplex models were initially proposed by Guttmann in 1954 as a "circular pattern of correlations in a matrix" [363] or a "system of variables which has a circular law of order" [364], visually resulting in a two-dimensional representation of a domain (such as an attacker landscape) in which a variable set is conceptually arranged as a circle [365][366]. These models have mostly found application in diverse clinical psychology and sociology contexts such as research on e.g. interpersonal traits and interactions; personality factors and disorders; mood and affect; family and marital systems or vocational interests (as reviewed in Gurtman & Pincus [364] and Acton & Revelle [367]). But classic circumplex models are far more than circular graphical visualisations describing a certain domain — they are statistically testable [367] against a number of criteria to assess their circumplex properties [365] and fit to underlying data [363]. Several criteria define circumplex models conceptually: firstly, they are best suited to accommodate two dimensions only and require interrelated variables as represented by a correlation coefficient matrix. A perfect circumplex is also signified by equal spacing of variables along the circumference of the circle and constant radius from the centre of the circle [365] and can be reviewed as such using statistical testing and simulation (as described by Acton & Revelle in their work on evaluating psychometric criteria for circumplex structures in [367])[51].

When it comes to adapting circumplexes as vehicles of representation for attacker categorisations, much weight is placed on the works of Rogers [46][23][368], in line with the overall development of literature around attacker typologies and taxonomies. While Rogers in [23] recognises that circumplexes have traditionally been used to model more complex, empirically-based behavioural concepts and personality traits as outlined above, he sees them primarily as a representation option to visually accommodate two interrelated variables (specifically attacker motivation and skill level) in contrast to a one-dimensional 'continuum' (two separate lines; one each for motivation and skill level). The circumplex as used by Rogers (refer to Figure 6.8 A on p.165) does not possess an attached correlation matrix defining "the exact relationship between classification variables" [23] or underlying statistical data to test against. It can therefore not be viewed as a testable and empirically based circumplex aligned with

[51] This paragraph offers a very brief introduction into theory around circumplex models, to help distinguish between the models as they are traditionally used and how research papers on attacker taxonomies have adopted them in their role as visualisation tools. The referenced works [363][364][365][366][367] provide detailed theoretical grounding and further references including examples for such models.

previous clinical psychology or sociology works as referenced above, it seems to merely be a visualisation tool referring back to the circumplex shape (Rogers indirectly acknowledges this in [23] by suggesting an examination using correlation coefficients as part of potential future research).

Guided by their intention to update Rogers' work, Hald & Pedersen [24] follow his approach largely uncritically, mapping their new attacker categories onto the original dimensions (see Figure 6.8 B) — also completely in line with Rogers, they view circumplexes as a "visualisation tool [...] designed as an aid in digital forensics to determine which category of hacker might have perpetrated an attack". Seebruck ([25]; Figure 6.8 C and D) acknowledges the origin of circumplexes as "adapted from psychology by sociologists seeking to classify groups according to attributes" ('dimensions' in Lindqvist & Jonsson in [25]). While he adapts circumplexes as an intuitive way of visualisation for attacker categorisations citing Rogers' work [23], he regards the way circumplexes have been used previously as problematic due to their inability to depict multiple, complex motivations in attackers. In these previous models (Figure 6.8 A and B), four quadrants represent four distinct types of attacker motivation — as every attacker node can only be placed into one quadrant (or across the border between two sectors), only one (or two) type(s) of attacker motivation can be represented. An additional visualisation in form of an 'arch' to add a third dimension (secondary motivations) to the circumplex is therefore suggested by Seebruck in [25] (as shown in Figure 6.8 D) — in the strictest sense, this invalidates this representation as a traditional circumplex as proposed by Guttman, but falls in line with the visualisation approach taken by Rogers and Hald & Pedersen taken previously.

While this alternative usage of the circumplex model representation in attacker categorisation literature is not necessarily a methodological shortcoming, using a term such as 'circumplex visualisation' or similar and an explanatory note referring back to circumplex theory may help to avoid ambiguity and strengthen the theoretical grounding for future attacker typologies and taxonomies relying on this method of visualisation. The next section considers the practical value and usefulness of such representations in current and future research using an example circumplex visualisation (compare to Figure 6.9 on p.166).

Based on the data-driven typology set out in this chapter, a new circumplex visualisation specific to digital banking attackers was created (Figure 6.9 on p.166). As an initial iteration of this circumplex visualisation, a four-quadrant structure as suggested by Rogers and Hald & Pedersen (compare to Figure 6.8 A and B) was adopted: four quadrants representing the primary four motivations for attackers (financial gain, ideology, challenge and revenge) are drawn to map the attacker's resource level — the further out the attacker type is placed on the radius of the circumplex, the higher their resource level. This chosen structure firstly ensured visual comparability to prior work, but most importantly visualised the three main motives encountered in the sample for digital banking (financial, ideology, challenge) plus revenge as an additional element potentially found in insiders. At this point, the arc representation proposed by Seebruck was not replicated as most attacker types in the set shown in Section 6.1 are defined by a single motivational factor. Together with the review of Figure 6.8 , the creation of the new circumplex as shown in Figure 6.9 helped to highlight several problems, but also positive aspects, for circumplex visualisations.

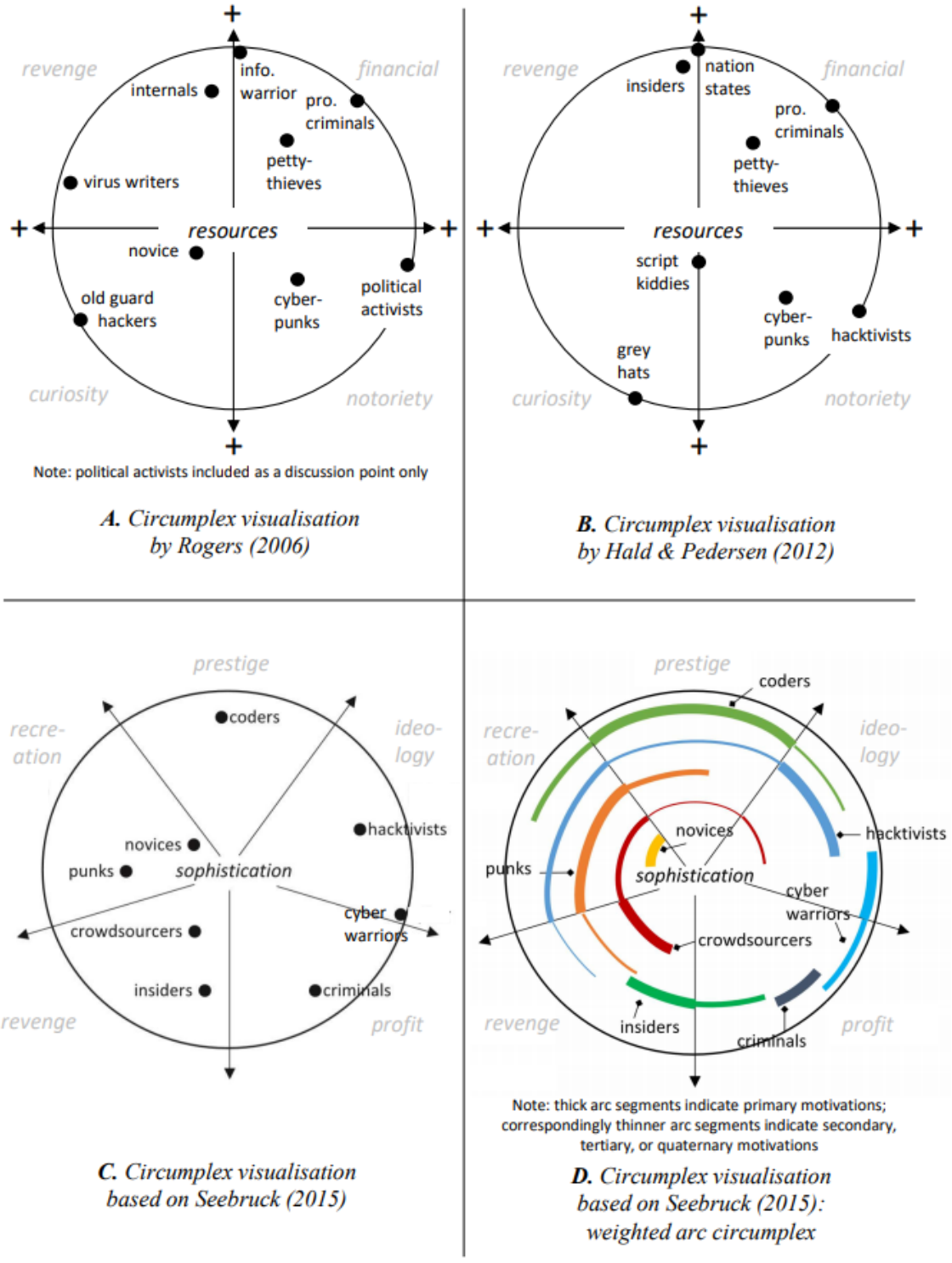


Figure 6.8: ***Overview of previous attacker circumplex visualisations (based on [23][24][25])***

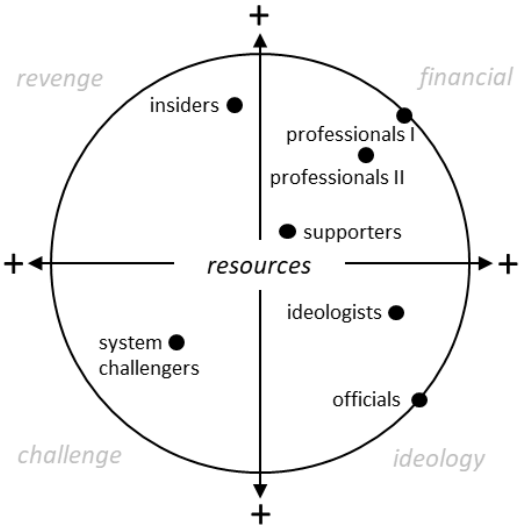


Figure 6.9: ***Circumplex visualisation for digital banking attacker typology***

In the context of attacker categorisations, circumplex visualisations could be viewed as problematic due to their:

- relative level of ambiguity and vagueness due to the manual mapping and positioning of categories/attacker types onto the circumplex;
- limitation to two classification dimensions as criticised by Seebruck [25];
- potential over-simplification of attacker landscape which may limit practical value to practitioners;
- stand-alone nature without link to existing threat modelling methods; and lastly
- lack of options for statistical testing and formal evaluation.

In contrast, they can be viewed as beneficial based on their:

- highly visual nature which should make them accessible to a wide range of stakeholders;
- ability to enable comparisons across typologies (by overlaying circumplexes using the same dimensions);
- potential to visualise the full attacker landscape and consideration of all relevant attacker types; and furthermore
- capability to illustrate the relationship between skills and motivation in attackers (as mentioned in Seebruck [25]); and
- potential usage as an investigative tool if individual attackers and case reports are mapped onto an existing circumplex (as suggested by Rogers [23]).

Reflecting on this excursus and the role of circumplex visualisations in attacker categorisations, the theoretical complexity and nature of traditional circumplex models as found in dedicated literature (compare to footnote on p.163) should firstly be acknowledged. In contrast, circumplex representations as used in attacker categorisations can be clearly distinguished here and be viewed as visualisation tools. This also explains their current value and

usefulness — they can serve as visual guidance to anyone interested in attacker landscapes and may help to see the 'big picture' including approximate skill levels, main motivation and other attacker types relevant to the domain. They are however only of limited use for more formal threat modelling approaches as they lack specific information on potential attack vectors and surfaces, making identification of threats difficult (as discussed in Section 2.2 and in Shostack [6] p.28) — this aspect is also included in the suggestions for future research directions in the next section.

6.4 Reflection

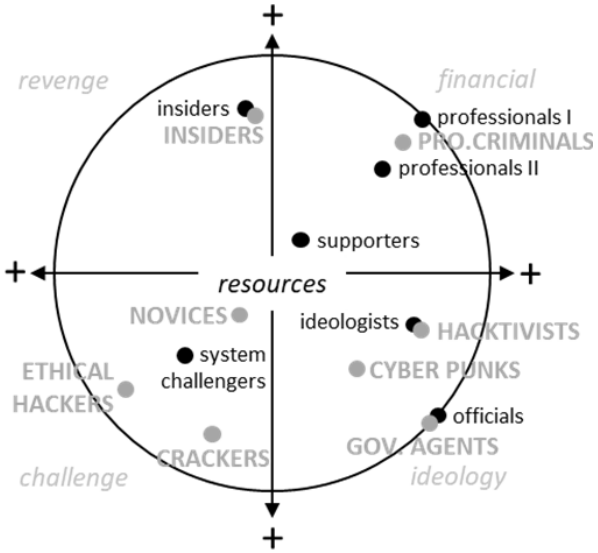
This discussion section reflects on the contributions made in this chapter, also putting these results into context with related literature in the domain of attacker categorisations. It begins with a comparison between the newly devised typology specific to digital banking and prior, general categorisations from literature. This is followed by a discussion of identified current limitations and lastly an enumeration of the future potential of attacker categorisations, also making a note on their perceived value for threat modelling.

6.4.1 Comparison with prior categorisations

For the purpose of comparing the new digital banking attacker typologies and prior categorisations, two research tasks were completed — firstly, the new attacker types were juxtaposed with the consolidated list of attacker types from previous literature as constructed in Table 2.3 in Section 2.3 (shown in Table 6.10). Secondly, a circumplex visualisation as introduced in Section 6.3 was used to visualise these differences: for this purpose, an approximation of existing attacker type categories is drawn out and superimposed onto the circumplex visualisation depicting the new typology for digital banking (in Figure 6.10, also Table 2.3).

New typology for digital banking	**Existing categories (see Table 2.3)**
System challengers	Novices Browsers and cyberpunks Crackers Ethical hackers
Insiders	Insiders
Supporters	—
Ideologists	Hacktivists
Officials	Government agents
Professionals I: groups and gangs	Professionals criminals
Professionals II: small groups and individuals	Professionals criminals

Table 6.10: ***Attacker types in new digital banking typology vs. existing attacker categories (consolidated)***



Note: Digital banking typology positions depicted using black circles, lower case labels; existing categories in grey and capitals.

Figure 6.10: ***Circumplex visualisation: comparison with previous attacker categorisations***

Table 6.10 and Figure 6.10 show the mapping of the new typology against existing categories. While some categories can be aligned easily (insiders, ideologists/hacktivists, officials/government officials), several differences can be noted: in our typology, a number of categories present in existing categorisations have been summarised under 'system challengers' — attackers in this group share the motive of wanting to overcome the security defences of a system rather than having a monetary interest. This consolidation also reflects the limited amount for references to such attackers found in the digital banking specific sample. In contrast, the professional criminals category in existing categorisations has been split into two categories to help represent and further explain some of the most common attacker types for digital banking — as noted in Table 6.6 and 6.7, these two categories are supported by a relatively larger amount of relevant references in the sample. Other differences are the lack of a supporters group in existing categorisations — these are specific to digital banking (for money mules for example).

Overall, the observed variances are in line with expectations when shifting the attention to digital banking attacks only: the increased focus on financially motivated attacks and higher number of professional criminals found in this context seem to justify the inclusion of two categories describing variations in professional criminals. It also justifies the limitation of system challengers and related attacker types to one category. This shift from an attacker set defined by various motives to an attacker set largely dominated by one type of motivation (financial gain) is particularly evident when comparing the new circumplex visualisation and consolidated attacker types from previous literature (Figure 6.10): the upper left quadrant accommodating financially motivated attackers is heavily occupied for the digital banking typology, while general categorisations include a larger number of attackers motivated by challenge or ideology (two lower quadrants). Both attacker categorisations in the circumplex show a similarly large spread for level of resources found in attacker types.

6.4.2 Limitations

Although several identified issues with the initial version of our digital banking typology have been addressed following the validation as per listing in Table 6.8, several limitations and constraints remain for the here presented next iteration. These can be roughly split into factors directly relating to the typology structure and contents itself, the circumplex as a chosen visualisation tool and lastly, environmental factors concerning the research area of attacker categorisations.

Firstly, and concerning the introduced typology itself, the following limiting aspects should be considered at this point in time:

- *Data sources underlying and informing this typology* — while care has been taken to use a considerably large and diverse data sample including information on digital banking attackers (see Section 3.4), additional data sources could help to provide further confidence, detail and opportunity for further development and adaptations to the typology on a continuous basis, also accommodating the changing threat and attacker landscape faced by digital banking over time.
- *Level of validation and triangulation carried out to date* — while the current iteration of this typology stems from the basic validation exercise as carried out in Section 6.2, further validation options should be integrated in subsequent iterations of the typology. A natural extension seems to be a larger scale validation using subject matter experts on digital banking security, but also the comparison to existing attacker categorisations (although the author is not aware of a directly comparable typology focussing on the banking sector at this point in time).
- *Content, structure and data richness across typology* — from a content perspective, the typology in its current iteration contains several elements based on either limited evidence (marked with * in Tables 6.1 to 6.7) or assumptions (marked with **); furthermore, the weighting of attacker categories is indicated in Tables 6.1 to 6.7, but not further accounted for; dimensions, their relevance and strict necessity are not evaluated in detail; and lastly, some dimensions may lack adequate detail or rigour to produce value to practitioners (e.g. activities/modus operandi). Here, working towards further typology iterations, using both additional and newly emerging data as well as validation feedback, could help to mitigate and improve on these aspects.

Secondly, circumplex models, when used in their function as visualisation tools in the context of attacker categorisations, require several cautions as discussed in Section 6.3: although highly accessible and replicable, their simplified, two-dimensional nature may restrict their value for real-world security assessments and threat modelling in practice.

Thirdly, this work only considers a very limited range of extension and visualisation options for attacker categorisations (i.e. circumplex models in line with prior research) at this point in time. Equally, the typology, while focussing on a relatively narrow context, is still generic and does not aim to integrate directly with existing risk or threat modelling methods. Both of these realisations open up new directions for future research and are applicable to the overall field of research rather than limited to this typology.

6.4.3 Potential directions for future research

In direct relation to the results presented in this chapter, the following further extensions are suggested for this digital banking typology, also based on the limitations presented in the last section:

- *Further refinement of specific attacker groups or other subcategories* — rather than creating new attacker categories for other applications, the digital banking typology or just certain categories (e.g. supporters/money mules) could be further refined and broken down into more subcategories and secondary attacker profiles. Further refinement could also prove useful to fully understand the nature of attackers specialising in a certain crime or using certain methods.
- *Further validation through expert reviews* — a selection of subject matter experts (for example financial services security personnel, law enforcement professionals or other practitioners as well as academics in the field) could provide further insight on the validity and completeness of the taxonomy. As these groups may also be the main beneficiaries or users of the taxonomy in their everyday work, receiving their feedback and insights would be valuable. A perspective on how thinking about attackers, also including attacker types and categorisations, is featured in the everyday work routine of banking professionals is given in Chapter 8.
- *Replication efforts with new data* — other data sources of digital banking fraud case reports could be used to replicate, test and subsequently adapt the defined attacker typology. As a validation approach followed by Hald & Pedersen in [24], assessing new real-world attacks against the categories defined could help to establish the explanatory power of a typology, expose potential gaps and address limitations around dimensions, weightings and overall data richness (see Section 6.4.2). But using new data sources to test the typology is also in the spirit of grounded theory research — continuous comparison against new data will help to improve, refine and keep the typology up to date.

Indicated by the results presented in this work, but also relevant to other works in the area, the following future topics of interest are suggested:

- *Alternative visualisation options* — visualisation approaches play a large role in the field of attacker typology research and are included in several key works, e.g. Rogers [23] or [42]. This work has provided a critical review of circumplexes as visualisation tools in the context of attacker categorisations and provided an initial example of a circumplex visualising digital banking attacker types. Following on from this review, new and alternative visualisation techniques not yet introduced into the context of attacker typologies should be evaluated, experimented with and adapted accordingly to progress this issue. Remaining with circumplexes, Seebruck [25] for example has suggested a more complex 'weighted arc circumplex model' accounting for multiple attacker motivations, which could potentially be adapted for the case of digital banking.
- *Attacker typologies for other industries* — much like a typology can be created from a dataset on digital banking, they can be created for a number of industries and ap-

plications, e.g. e-commerce or for very specific cases (Nurse et al. use the example of insiders targeting intellectual property in [369]).

- *Research into potential extensions and integrations* — further research into extending and integrating attacker categorisations with existing methodologies in an organisational and academic context would be of potential benefit, to overcome the relative 'stand-alone' nature of attacker typologies and taxonomies. This could include examinations around the practical value and fit of attacker categorisations for organisations and their everyday practices. As an example, models used in organisations such as the cyber kill chain (as introduced on p.28).
- *Further enquiry into the human nature of attackers* — Atzeni et al. [7] or Faily & Fléchais [27] have proposed the creation of attacker personas to realistically represent archetypes of attacker types, providing detail-rich, fictional attacker profiles including biographical details and narratives. Similarly, Mead et al. introduced their 'persona non grata' as part of their hybrid threat modelling method in [14]. While these representations are in contrast to the factual high-level description achieved by the attacker typology presented in this chapter, these could form a grounded basis to create a range of attacker personas with the aim of 'bringing to life' the humans behind attacks against digital banking systems. This idea is taken forward in Chapter 7, where an attacker persona set for digital banking systems is proposed using the attacker types presented in this chapter and evaluated for its usefulness with financial services professionals.
- *Relationship with threat modelling and attacker-centric security* — as suggested by Shostack in [6] and introduced in the introduction and background section of this thesis (Section 2.2), software- and asset-centric approaches (rather than attacker-centric) are usually preferred in the threat modelling domain. The discussion on the role of attacker representations is expanded on in Chapter 8, where attacker-centric security and thinking about attackers as observed by security professionals in banking is explored.

6.5 Conclusion

Summarising on this chapter, an attacker typology including seven distinct attacker types relevant to digital banking has been identified from the analysed dataset, following the research procedures as set out in Section 3.5.2 and building on the grounded theory data analysis as presented in Chapters 4 and 5. Following amendments made after an evaluation exercise in Section 6.2, this current version forms the second iteration of the attacker typology, with the initial version published as [275] previously.

While the work presented in this chapter should be considered as tightly integrated with previous key works (as reviewed in Section 2.3), it has also aimed to challenge aspects found in prior works, such as the largely uncritical usage of circumplex models in e.g. Rogers [23] or Hald & Pedersen [24]. Furthermore, limitations identified for this work, but also inherent to the research domain have been acknowledged, potentially encouraging future iterations of the here presented or similar typologies in the future.

It is also hoped that this work will contribute to the overall research domain of attacker categorisations, showcasing an interesting area of research, but also highlighting currently prevalent issues warranting future research. Beyond adding another categorisation in the form of a typology to the bulk of research for comparison and reference by others, the excursus on circumplexes and validation examples may be of particular value of others.

Lastly, the introduced typology also serves as a basis for the following chapter, picking up on the aspect of extending the relatively factual attacker profiles into a more human, near-realistic representation of archetypical digital banking attackers via the persona method, building on works for example by Mead et al. [14] and Atzeni et al. [7]. Here, the attacker typology is used within the research procedures to build the personas following a user-centred design method based on a 10-step method devised by Nielsen in [29], forming an initial draft for the attacker persona set to work on. This chapter also prepares for Chapter 8, which discusses attacker-centric security approaches with digital banking professionals. In this context, the typology forms a substantiated discussion basis for the researcher to base semi-structured interviews and conversations on, making references to individual attacker types within the typology where useful.

Personas, like all powerful tools, can be grasped in an instant but can take months or years to master.

— Alan Cooper,
The Origin of Personas
cooper.com, 2008

7

Attacker Personas for Digital Banking

Directly building on the attacker typology introduced in the last chapter and analysis undertaken in Part II, this chapter proposes a set of seven attacker personas specific to digital banking as an attacker-centric tool, using a 10-step process model borrowed from user-centred design as a construction method. To document the results, each attacker persona is represented by a detailed profile card and a long-form narrative story. Following the process model, an evaluation exercise in the form of a survey study with 85 financial services practitioners is undertaken, followed by a concluding discussion.

The potential usefulness of persona representations for areas outside of user-centred design, where personas are traditionally used to represent a range of legitimate and task-driven system users, has been recognised by several authors in the past, also in information security. As introduced in the background section of this thesis in Section 2.4, Steele & Jia [44] brought personas into the security space by proposing 'adversary-centred design' using anti-scenarios, anti-use cases and anti-personas. The term 'attacker personas' was further developed in Atzeni et al. [7] with their approach to creating and using attacker personas in a project setting. Outside of the security community, Bødker & Klokmose [277] have since introduced the idea of a 'techsona' to extend the persona and scenario concept with a matching technology counterpart.

To date however, methodological advancement for attacker personas and interest from secu-

rity professionals for attacker personas have been limited as argued in Section 2.4: very few end-to-end examples of attacker personas have been built and presented in detail for specific real-life settings or applications — attacker persona research (e.g. [7][27][44][45][60][120]) has often been restricted (due to constraints in space or focus) to showing only limited examples and excerpts rather than full attacker persona sets.

Additionally, from a conceptual point of view, the integration of human adversary representations like attacker personas into formal and informal security assessments does not seem to be adequately established at this point in time, also evidenced by limited documentation of practitioner usage — while e.g. Shostack includes examples of attacker personas in the appendix of his key textbook on threat modelling [6] p.480, their direct integration into threat modelling approaches for practitioners remains vague. In contrast, Faily provides a thorough and structured integration of the persona method into usable security design processes through their *IRIS* framework and the *CAIRIS* platform in [96], showing the vast potential personas may offer if they can be integrated into existing or newly adopted organisational procedures and work routines.

As set out in Sections 1.3 and 1.5, two main objectives and expected contributions can therefore be identified for this study: firstly, to construct a complete attacker persona set (using the specific case of digital banking as a case example) in order to complement existing research in this area; and secondly, to help establish the practical value and (future) use of such an attacker-centric tool amongst financial services practitioners. To achieve this, a comprehensive construction method for conventional user personas (by Lene Nielsen in [29][30]) has been selected and detailed in the research procedures in Section 3.5.3. In the context of the overall thesis, this study makes use of the attacker typology from Chapter 6 as an initial draft for the attacker persona types, while attacker personas are also considered in the conversations with practitioners in Chapter 8.

This chapter is structured in alignment with the 10-step process model steps proposed by Nielsen [29][30] as prepositioned in the research procedures in Section 3.5.3, specifically in Table 3.10 on p.83. Initially, any preparations for persona construction including data collection and proposal of a first draft are set out. This is followed by the results section, providing an overview of all personas in the set, including their hierarchical order. Next, an evaluation of the new attacker persona is undertaken using a survey study amongst financial services practitioners, also leading to several amendments to the initial attacker persona set. This is continued with a discussion of positive and negative implications of attacker personas identified during the research process, followed by a note on their continuous and future development as well as a brief reflective conclusion. To supplement this chapter, Appendix A includes seven narrative stories to be viewed alongside the persona profile cards.

7.1 Preparing for attacker persona design

In preparation for the presentation of results in this chapter (in the form of a full attacker persona set for digital banking), three essential research tasks are initially carried out — these are described in turn in this section.

Firstly, the process of transforming the data collected, analysed and synthesised from an attacker typology (in Chapters 4 to 6) into attacker personas is commented on, in alignment with Nielsen's process model steps 1 to 3 (refer to Section 3.5.3 for the full process model and its steps). Secondly, to help establish the overall structure and weight every persona carries within the set, a hierarchy of three different attacker persona types is proposed — this element corresponds to process model step 4. Thirdly and lastly, to document the attacker personas created in the best way possible, the intended way of presenting the individual attacker personas is outlined. While a number of visualisation and dissemination options are available and discussed in traditional persona literature (in Nielsen's work, but also in e.g. Adlin & Pruitt's *The Essential Persona Lifecycle* [28]; or Pruitt & Grudin: *Personas: Practice and Theory* [302]), 'persona profile cards' are chosen to represent the attacker personas and their situation ('biography') within this thesis — this element is aligned to both process model steps 5 and 6, with an additional reference to step 9 in regard to narrative scenarios.

7.1.1 From data to personas

The basis of Nielsen's 10-step process model for creating personas [29][30] is formed by a data collection process, a first draft made up of different persona types and lastly a review of these initial findings (steps 1 to 3; pp.82). As a data collection and analysis process relevant to characteristics and behaviours of digital banking attackers has already been undertaken in detail in Chapters 4 and 5 (process model step 1), with an attacker typology serving as an initial draft of attacker types created in Chapter 6 ('hypothesis' in Nielsen; process model step 2), this section describes how these existing starting points have been transformed into an attacker persona set.

To start, and in alignment with process model step 3, the attacker typology as an initial draft of seven attacker types is to be examined and supplemented with further detail to help prepare the creation of an attacker persona set. For this purpose, the original materials used to construct the typology (in the case of this thesis, the data sources described in Section 3.4) should be re-checked and reviewed in further detail against a set of properties for their potential value to inform the personas. Here, Nielsen originally proposes several properties applicable to user personas in [29] (see also Section 3.5.3), which can be adapted accordingly for a security context and attacker personas:

- For attacker persona descriptions, information on potential motives and intrinsic motivations displayed by attackers as well as their values and moral code should be considered.
- For attacker persona situations, information on the attacker's external and social circumstances should be added, e.g. their available resources, occupation or living situation.
- For attacker persona scenarios, information on potential attacks as well as related factors (e.g. the attacker's path into crime) could be of use.

Using this list, the original source dataset was re-checked to add these aspects to the attacker types found in the attacker typology. Additionally, another review of the dataset looking

for basic attacker characteristics, behaviours, activities and other narrative snippets in alignment with the seven draft attacker types was carried out to ensure all information had been captured. Lastly, personal quotes from attackers were collected where available. With this information added, the seven attacker types were now ready to be assembled into a structured persona set and visualised as detailed human attacker profiles.

7.1.2 Introducing persona hierarchy

To help account for the relative importance and impact every attacker persona is expected to have on the setting they are placed in (i.e. digital banking in this thesis), the introduction of different types of attacker personas is proposed, in line with suggestions for traditional user personas in user-centric design theory [30][372][278]. Loosely based on persona types used for user personas (in Cooper [278] pp.104), the implementation of three different types of attacker personas seems beneficial. These three types are defined by their overall importance and relevance to digital banking systems, but they also specify how much of the threat landscape is covered by the respective persona.

1. *Primary attacker persona* — a primary attacker persona (or a group of primary attacker personas) usually represents the bulk of attackers and attack variations and is responsible for most of the potential attacks to a system. For this reason, it most likely forms the primary focus for security design and mitigations in place.

2. *Secondary attacker persona* — a secondary attacker persona represents different, but nevertheless important attacker motivations and attack scenarios that are not covered by the primary attacker personas. However, the security design and mitigations in place (for primary attacker personas) mostly protect against them and their attacks.

3. *Supplemental attacker persona* — supplemental attacker personas present other attacker types commonly found in the reference dataset — their attacks should already be mitigated by protecting against primary and secondary attacker personas. While they are not necessarily useful for security design, they nevertheless represent realistic attacker portraits from the data and will help stakeholders to gain a full picture of the range of encountered attackers and their relevance for security design (based on Goodwin [372] p.275).

In short, protecting against primary attacker personas will provide mitigations against most attacks to a system. However, secondary and supplemental attacker personas still add value — first and foremost to enable a validation of the assumption that mitigating against primary attacker personas will indeed cover the full range of known threats and attacks to a system. They also ensure that a convincing and realistic picture of the overall attacker range can be presented to stakeholders. In some cases, attack patterns may change over time and secondary or supplemental attacker personas may become a primary threat to a system. The hierarchical structure for attacker personas may also be influenced by the focus defined by the security team in an organisation (e.g. certain attacks have increased and should be addressed as a priority). On the other hand, the attacker persona set and its hierarchy may help to decide where to focus efforts.

7.1.3 Format of presentation

In traditional persona design, a multitude of persona materials are used to communicate and disseminate the personas across the organisation, making it usable and referable from the moment they are "released into the wild" [28]. In their central work on persona usage in theory and practice at Microsoft, Pruitt & Grudin [302] describe the creation of "variations of posters, flyers, handouts and a few gimmicky promotional items (e.g. squeeze toys, beer glasses, mouse pads — all sprinkled with persona images and information)". Previous research on attacker personas has generally made use of simpler representations, like one page overviews (also in electronic form) including key information on the fictitious attackers (e.g. [7][27][44][60]).

In line with this previous research and to accommodate the largely corporate audience for the attacker personas introduced in this thesis, 'attacker persona profile cards' are chosen as the main way of communicating and disseminating the individual attacker personas and the overall set (Figures 7.2 to 7.8). These single-page overviews use a clear structure and design and include both a basic description and brief biography of each attacker persona — they can be used in an electronic format (e.g. to be sent as an email attachment or to be placed on the internet or intranet, which is how they have been used in the context of the evaluation study in Section 7.3) or as physical print-outs.

Following the persona creation guidelines from Nielsen [29][30], each attacker persona first received basic properties such as a name, alias where meaningful, age and location. While the individual elements including the short biography are fictious, they are based on real data and grounded in the dataset underlying this thesis (e.g. age or education; Sections 4.1.1 and 4.1.3 respectively). The profile picture for each attacker persona was also carefully chosen at this point, using a stock photography database [373]. While the biography element includes information on the current situation an attacker persona is in, more details on their situation and 'story' are provided in the extended scenario narratives (as included in Appendix A; refer to Section 7.2.3).

7.2 Results

Following directly on from the last section, this section presents the results from the construction of an attacker persona set relevant to digital banking, following Nielsen's 10-step process model as set out in Section 3.5.3. Initially, the overall structure of the attacker persona set is described, listing the contained personas and their hierarchical order. This is followed by the presentation of seven attacker persona profile cards for each individual persona in the set (Figures 7.2 to 7.8). Lastly, narrative scenarios, which complement each attacker persona and are included in Appendix A, are explained in further detail, concluding this results section in preparation for the evaluation exercise for this attacker persona set in Section 7.2.3.

7.2.1 Attacker persona types for digital banking

From the seven initial attacker types defined in our typology in Chapter 6, seven attacker personas at three hierarchy levels are proposed (for an overview, refer to Figure 7.1). Most

Figure 7.1: ***Overview of complete attacker persona set***
(profile picture photographs: Getty Images/iStock [373])

crucially, the ideologists and officials categories have been merged, while the systems challengers category has been split into two attacker personas (with the addition of the 'security researcher' persona). Additionally, the supporter category has been included as the 'money mule' persona. Further amendments to the initial hypothesis of attacker types (based on the attacker typology) and all proposed attacker personas are explained in the remainder of this section.

Primary attacker personas

- Professionals I: large groups and gangs
- Professionals II: small groups and individuals (including toolkit users)
- Insiders

Attackers in large groups and gangs were selected as a primary attacker persona as protecting against them, with their high criminal intent and financial gains motivation paired with an advanced level of skills and resources, should cover a wide range of attacks against digital banking systems. Small groups and individuals were then selected as a primary attacker persona as advanced social engineering, very specialised or locally targeted attacks may be used by this group. Their inclusion is justified as these attacks and the employed modus operandi may slightly differ from larger groups and gangs. In line with the changes made for the second iteration of the attacker typology in Chapter 6, toolkit users are not represented by their own attacker persona — they are also covered by mitigations for the other primary attacker personas. Lastly, insiders were also selected as a primary attacker persona as insider threats and attackers on the inside may require specific mitigations and would not be covered by the other two (external) primary attacker personas.

Secondary attacker personas

- System challengers
- Ideologists and officials

Two secondary attacker personas were also selected as these attacker types differ significantly from the primary attacker personas, mainly in regard to their motives — financial gain is not a primary motivator for these two attacker types. System challengers covering a wide range of attackers with varying levels of resources may pose a threat to digital banking systems, but their attacks are usually mitigated by protecting against financially motivated primary attacker personas. Ideologists and officials were combined into one attacker persona to represent their relatively small weighting in the attacker persona set — while both attacker types are relevant to banking, not many attacks are known to date or could be found in the analysed dataset.

Supplemental attacker personas

- Money mules
- Security researchers/ethical hackers

In line with the proposal on persona hierarchies in Section 7.1.2 based on the persona types from Cooper [278] and also Goodwin [372], two supplemental attacker personas were added at this early stage of the research (with the assumption that these may change). Money mules (originating from the supporter category from Chapter 6) account for a large number of coded references in the original dataset and hence were expected to play a significant role in digital banking fraud. It therefore made sense to add them as a supplemental attacker persona to create a comprehensive attacker persona set which will convince both stakeholders and subject matter experts. The addition of security researchers/ethical hackers (extracted from the system challengers category from Section 6.3) as a supplemental attacker persona was based on a similar rationale. While no separate defence mechanisms are needed to protect against them, they still play a role as mostly 'friendly' attackers in the security ecosystem around digital banking, trying to help to improve security through their actions rather than cause harm. This may for example take place through responsible disclosure schemes or bug bounty programmes that several banks are using now, e.g. Royal Bank of Scotland in the UK [361] or ING Groep in the Netherlands [374].

7.2.2 Attacker persona profile cards

Following the overview of the attacker persona set introduced in the last section, the profile cards for each of the seven proposed attacker personas are shown overleaf in Figures 7.2 to 7.8.

BRUNO – the gang leader

GROUP: PROFESSIONALS I: Groups and Gangs

TYPE: Primary Persona

NAME Bruno
ALIAS S0ld1er
AGE 28
LOCATION Believed to be in Russia – has ties to Sweden and Eastern Europe, also seen in Thailand

"I ran the organisation as a business, employing a director of marketing, a website developer, a customer service manager [...]"

MOTIVES

- Financial gain
- Luxurious lifestyle

ACTIVITIES & MODUS OPERANDI

- Large-scale malware attacks
- System intrusion
- Attack innovation – involved in devising new attack types as he has the best hackers working with him
- Criminal-to-criminal sideline business: hacking kits for banking trojan
- 'team leader' – responsible for controlling and organising the group as well as recruiting

LEVEL OF RESOURCE

Skills

Equipment

Funding

BIO

A true maths genius and talented computer programmer, Bruno decided to turn to cybercrime due to lack of legal employment opportunities giving him a good income. He's a natural risk-taker - but he knows that the risk of being caught is relatively low in comparison to the potential gains to be made.

Originally from Russia, he has long been hiding from law enforcement and not much is known about his personal circumstances.

Intelligent but ruthless, he is a charismatic leader with a business mind. He knows how to recruit and gather the best around him, but expects a lot and trusts no-one but a few loyal accomplices in his inner circle.

He is a professional criminal through and through. It's not that he has no ethics or morals – it's just that they are very different to the majority of the population.

CRIMINAL INTENT

Low — High

LEVEL OF DAMAGE CAUSED

Low — High

Figure 7.2: ***Attacker persona profile card for Bruno, the gang leader*** *(profile picture: Getty Images/iStock [373])*

Figure 7.3: ***Attacker persona profile card for Victor, the cyber thief*** *(profile picture: Getty Images/iStock [373])*

Figure 7.4: ***Attacker persona profile card for Allie, the insider informant*** *(profile picture: Getty Images/iStock [373])*

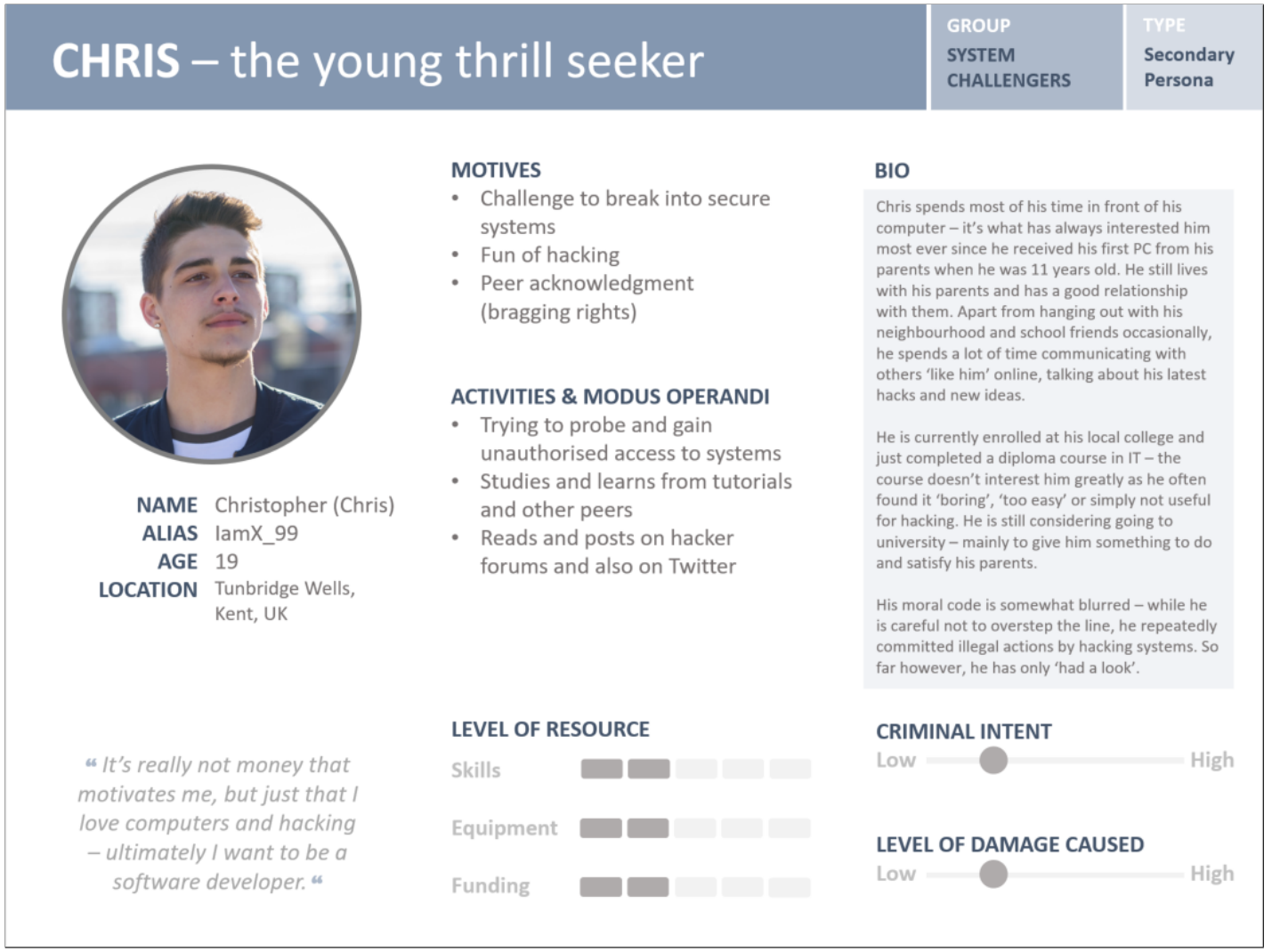


Figure 7.5: ***Attacker persona profile card for Chris, the young thrill seeker*** *(profile picture: Getty Images/iStock [373])*

AZ – the hacktivist

GROUP
IDEOLOGISTS & OFFICIALS

TYPE
Secondary Persona

NAME Asif (Az)
ALIAS Red Dragon
AGE 24
LOCATION Unknown

“I was inspired by the Anonymous movement to believe that every single person has the ability to make a change...“

MOTIVES

- Cause & ideology
- Create a new world, change things
- Believes in freedom of information for all and no copyright

ACTIVITIES & MODUS OPERANDI

- Will participate in large-scale DDoS attacks or breaking into systems of companies that have been identified as targets
- Continuous upskilling and learning
- Communicates with peers, using open and closed channels (IRC)
- Uses Twitter for communicating with the public

LEVEL OF RESOURCE

Skills
Equipment
Funding

BIO

Az is an activist who feels strongly about justice and equality – he believes in action rather than words alone and his aim in life is to make a difference. He is enrolled as a student for electrical engineering in the UK. He has had a keen interest in computers and has been hacking for years.

He is sociable with friends and likes to connect with others who feel strongly about something, from political activism to human rights to environmental issues or animal rights. He enjoys travelling and works from anywhere in the world. He likes being part of a group that believes in similar things.

Az’s moral values differ from conventional ones – he has no respect for large corporations or even government agencies. He doesn’t trust banks or payment providers and sees them as an enabler of things he is strongly opposed to like war or fracking.

CRIMINAL INTENT

Low — High

LEVEL OF DAMAGE CAUSED

Low — High

Figure 7.6: ***Attacker persona profile card for Az, the hacktivist***
(profile picture: Getty Images/iStock [373])

Figure 7.7: ***Attacker persona profile card for Kev, the money mule***
(profile picture: Getty Images/iStock [373])

Figure 7.8: ***Attacker persona profile card for Scott, the security researcher*** *(profile picture: Getty Images/iStock [373])*

7.2.3 Narrative stories for attacker personas

Placing the new attacker personas into the context of a narrative scenario is a key part of their creation (as prepositioned in process model step 9; p.85). After all, only a scenario links the attacker personas with an attack, targets or the relationship of attackers with law enforcement or other criminals (also in larger group settings). Bødker & Christiansen describe the creation of scenarios as a creative process and see them as "hypotheses, or qualified guesses about the artefact and its use" [301]. How then is a credible and authentic scenario best built? Nielsen [375] was left unsatisfied in her research on scenarios: "I was surprised to find that the scenarios never presented the users as vivid characters. At best they were stereotypes and made me laugh, at worst they only existed as a name". Her recommendation — based on the thorough review of scenarios in [157][376] and in the context of film scriptwriting — is to describe the user (or attacker in the case of this work) as a rounded character and avoid stereotypes. Furthermore, she states the importance that should be paid to the users' surroundings as well as the character traits, goals and tasks which characterise the users.

Nielsen describe scenarios and stories in great detail in [30] ch.9 — this reference was used as basis to build the narrative scenarios for the attacker personas in this chapter. They have been placed in the appendix of this thesis (Appendix A), mainly due to their relatively large size, but also based on the fact that they are not strictly required to form a coherent argument in this chapter. However, as they are seen to add further depth and interest to the attacker personas, are an integral part of Nielsen's model and have not been presented commonly in previous literature (as argued in the background section in Section 2.4), they have ultimately been included in this work.

There is one significant difficulty for this study and the writing of scenarios — the original data sources used (as defined in Chapter 3.4 and presented in Appendix B) do not always provide many details around character traits or characteristics outside the ones directly related to the attack committed. To help with this issue, data snippets from different sources are merged into one attacker scenario where considered helpful. An example is the usage of attacker information snippets ("he enjoys fishing"; "he was travelling when he was arrested at Nice airport") which are related to different attackers in the same scenario story. This technique of merging information is therefore seen to help to achieve a more dense, varied and realistic description grounded in data. Secondly, a small number of materials in line with the original dataset are added to help shape the scenarios (as described in Section 3.4.3 on additional data sources), with fictional story snippets added where required — however, main events and storylines are kept as close as possible to facts found in the dataset.

The scenarios — just like the attacker personas themselves — need careful and detailed reviewing with subject matter experts and stakeholders to ensure they are coherent, logical and ultimately convincing and useful to them. As with the descriptions of the attacker personas, the scenarios are not intended to be static, final stories. They will have to undergo regular checking and updating to reflect attacks against digital banking, the involved attackers and their activities realistically and accurately. They are therefore part of the materials presented to financial services professionals in the evaluation exercise and survey study reported on in the next section.

7.3 Evaluation: attacker persona perception (survey study)

To help evaluate and disseminate the new attacker persona set (as prescribed in steps 7 and 8 of the process model; p.84), a survey study was carried out amongst 85 financial services practitioners[52]. This study looked at the perception and value of attacker personas, both specifically for the persona set introduced in this thesis, but also regarding the overall value of the method where possible. In preparation of this, Section 3.5.3 has introduced the full research procedures and research decisions underlying this study, while Appendix C includes the participant sheet used in the ethics approval process and Appendix D shows the exact survey contents and question statements.

The concept of personas was known to just under half of the participants (39; 45.88%; Question Q3), while only 20% (17) stated they were aware of "the concept of attacker personas (or other similar representations of human adversaries)" (Q4). 73% of participants answered all questions, with people taking between under 10 minutes to over an hour to look at the attacker personas and to answer the questions. There was a drop-off point within the survey, where a number of participants (16) decided not to progress past the screens showing the attacker persona profiles (Appendix D). Overall however, internal validity of the survey as expressed by Cronbach's alpha seems given (see next Section 7.5.1) and a number of interesting and actionable feedback items were received to improve on the attacker personas (see Section 7.3.3).

Following the note on internal validity as mentioned, the results reporting in this section is structured around the five thematic constructs used for evaluating persona perception (originally based on Salminen et al. [289] and introduced in Section 3.5.3 p.86): clarity & presentation of the attacker personas as perceived by the practitioners, their completeness & consistency, credibility & empathy factors, perceived relevance & applicability as well as usefulness & willingness to adopt this method. Additionally, a note is made on any other practitioner input and feedback received outside of these constructs. These outcomes are then further reflected on and integrated in the discussion in Section 7.3.3.

7.3.1 Establishing internal validity (Cronbach's alpha)

Analysis for internal validity and consistency of the survey was carried out using Cronbach's alpha (α) as a coefficient of reliability (refer to Section 3.5.3 p.86). Cronbach's alpha indicated acceptable reliability for the survey study across all constructs, with all α exceeding 0.7 as a cut-off range for acceptability [312][377] as shown in Table 7.1. However, the removal of several problematic variables potentially including unreliable results was required to meet

[52]Within the sample of financial services practitioners who choose to participate in the survey study (N=85), 16.5% (14) of participants identified as senior managers or executives as their primary role, 28.2% (24) as managers, 23.5% (20) as analysts, 22.4% (19) as specialists or subject matter experts and 9.5% (8) as other, e.g. developer, designer, tester or solution architect (from Q1 in the survey). In terms of area of work or expertise participants identified with the most (with multiple answers possible), most participants (52.9%; 45) identified with the term security (including cyber, physical and corporate security), followed by digital (38.8%; 33) and business functions (35.3%; 30), consulting (29.4%; 25), risk (23.5%; 20) and fraud (20.0%; 17) and others (11.8%; 10), e.g. analytics, software development or project management (Q2).

Construct	α	Note
Clarity of the personas	0.877	
Completeness & consistency	0.712	Following suggested removal of Q13 (moved), 14 and 15
Credibility & empathy	0.788	
Relevance & applicability	0.709	Following suggested removal of Q23 and addition of Q13
Usefulness & willingness	0.819	

Table 7.1: ***Cronbach's alpha for survey constructs***

this threshold: in the completeness & consistency construct, both questions Q14 and Q15 ("Additional real-life situations and scenarios would have been useful" and "Additional information on how the personas may affect customers of this organisation (and their customer journeys) would have been useful") had to be removed, with results not in line with other questions in the same construct and therefore significantly lowering α. In the same construct, Question 13 ("The personas seemed very generic to me") seemed to affect α negatively, but was found to align — logically and statistically — with the relevance & applicability construct and was therefore moved across to be retained for results reporting. Lastly, Q23 ("I wish the personas were more tailored to my organisation or industry") significantly decreased α for the relevance & applicability construct and was therefore removed from further analysis. All other variables showed a decrease in α if deleted, hence indicating that they should be retained at this point and form the basis for the reporting of results in the next sections.

7.3.2 Results: five constructs of attacker persona perception

Using the five thematic fields and constructs the survey questions were grouped under (refer to Figure 7.9) as a structure, this section summarises the results from the study, providing insight on how financial services practitioners viewed the attacker personas introduced within this thesis and beyond as a general attacker-centric method in security. The five constructs align to Questions Q5 to Q31 of the survey, all containing statements to be rated against a 5-point Likert scale by the participants as set out in the research procedures in Section 3.5.3 previously. Note that Q1 to Q4 established basic information such as the participant's role, area of expertise and familiarity with personas as included in the introduction of this section.

In addition to the quantitative data collected around the constructs, participants were also given the opportunity to provide any other feedback at the end or even after completing the survey, using a free-text field (Q32), the researcher's contact email or by commenting on the intranet post including this survey (within the participating organisation only). 20 data snippets were collected in this manner and analysed separately (as mentioned in the research procedures in Section 3.5.3 p.86) — an excerpt of participant quotes illustrating the type of feedback received is shown in Figure 7.10. This input can be divided into two categories: feedback of more general nature, concerning attacker personas as a method overall (included at the end of this section), and feedback specific to our attacker persona set (presented separately in the next section, Section 7.3.3).

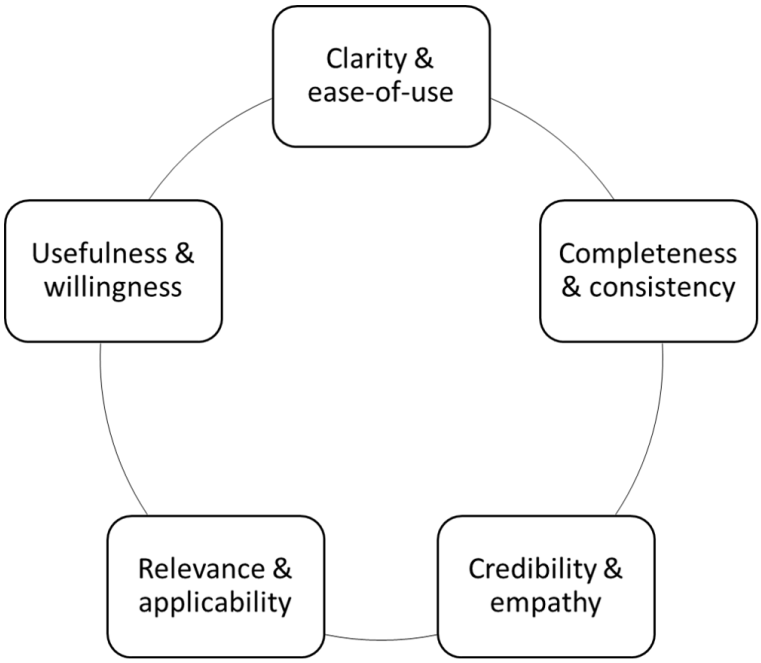


Figure 7.9: ***Persona perception constructs (based on Salminen et al. [289])***

Following this introduction, the results from the survey study can be summarised as follows around the five constructs:

Clarity & ease-of-use — Practitioners had viewed an overview of the attacker persona set and three example attacker personas (Bruno, Kev and Scott from the set in Section 7.2.2) at this point, with 69 practitioners scoring the statements on general clarity and perceived ease-of-use of the attacker personas within this first construct of attacker persona perception. The majority of participants rated the attacker personas as "easy to read and understand" (Q5), with 89.9% (62) agreeing or strongly agreeing with this statement — similarly, the short biography section (Q6) and the overall attacker persona set (Q7) were viewed positively by 94.2% (65) and 88.4% (61) of participants respectively. While these high scores support the easily accessible nature of the attacker personas, over 20% of participants (20.3%; 14) were not sure what the "persona method is trying to achieve" (Q9) — although this meant that nearly 80% of participants (55) were confident that they understood this aspect. Lastly, most participants (84.0%; 58) agreed or strongly agreed that they "enjoyed looking at the persona set and reading through the persona profiles" (Q8), highlighting the very positive first impression that the attacker personas had on the practitioners. This is particularly interesting given that only 20% of all participants were familiar with the method before commencing the survey (Q4).

Completeness & consistency — This second construct looked specifically at the attacker persona profile cards, asking for views on content and representation, with 66 practitioners scoring at least some of these statements. Initially, views on the value of additional real-life situations and scenarios related to the personas as well as their influence on customers and their digital journey were invited (Q14 and Q15) — however, these were omitted due to potential reliability issues indicated by Cronbach's alpha. These two questions may have been poorly understood or not been viewed as relevant by some of the practitioners, indicated by over 40% of participants (40.6%; 26 out of 64 valid responses) neither agreeing or disagree-

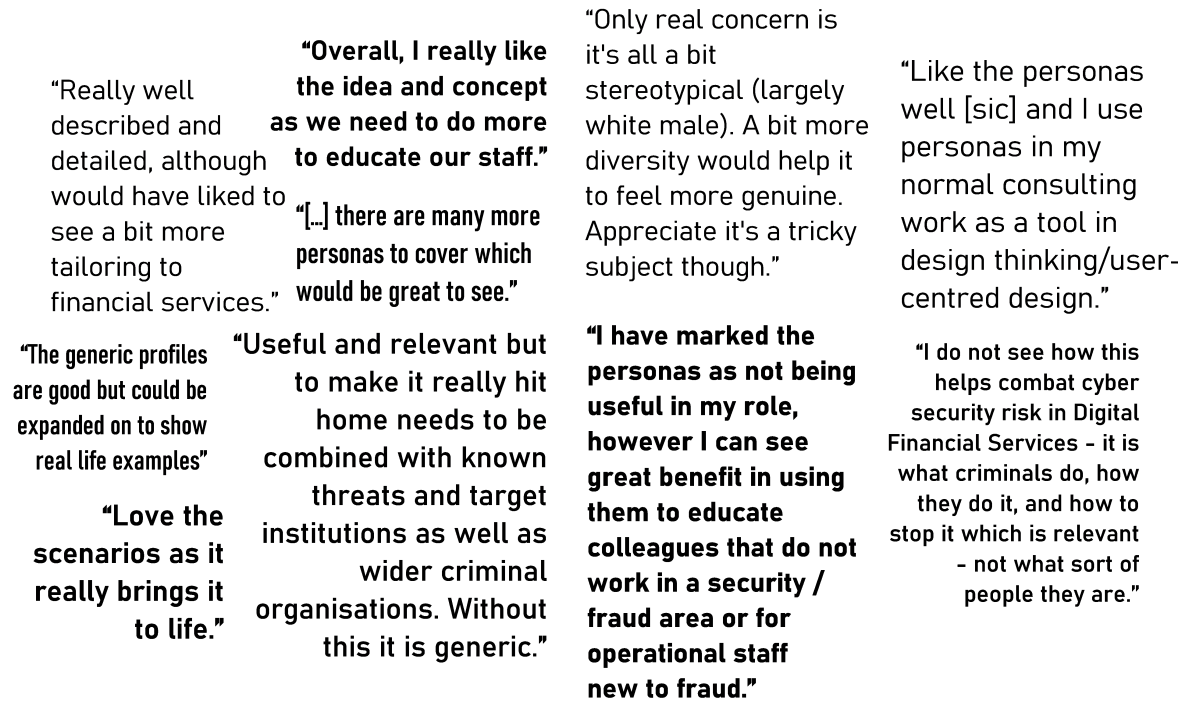


Figure 7.10: ***Selection of survey participant quotes: general persona perception***

ing/agreeing with the statement in Q14: "additional real-life situations and scenarios would have been useful" — these are therefore not considered in further analysis.

Overall, practitioners accepted the attacker persona profile cards readily, with only a minority disagreeing/strongly disagreeing (6.2%; 4 out of 65 valid responses) and 64.6% (42/65) agreeing that the names and ages of the example attacker personas and their descriptions were a good match (Q12) — however, 29.2% (19/65) were undecided at this point, hinting at the challenge of describing personas in a way that is suitable for all. The profile picture match (Q11) was not viewed favourably, with 16.9% of participants (11/65) disagreeing/strongly disagreeing on them fitting the descriptions well and 43.1% (28/65) neither disagreeing or agreeing in this context, further underlining the difficulty around choosing persona characteristics during the design stage. Similarly, while many participants (72.7%; 48/66) viewed the information provided on the personas as "plenty" (Q10), over one quarter disagreed or were not decided on this (27.3%; 18/66), showing the different viewpoints taken when looking at the same attacker persona set.

Credibility & empathy — The third construct intended to measure how convincing, realistic and credible practitioners would perceive the attacker personas — 64 participants attempted the questions in this construct. Most of them were confident that the attacker personas matched attacker types they had heard of before, in either media (Q16; agree/strongly agree: 79.7%; 51) or an industry context (Q17; 71.9%; 46). The response was more diverse when it came to attacker types they had encountered in relation to the organisation they worked in (Q18): here, 42.2% (27) neither disagreed or agreed on the attacker personas matching these attacker types, with around one third disagreeing (32.8%; 21; with 10.9% or 7 participants even strongly disagreeing) and only 25% (16) agreeing/strongly agreeing that our attacker personas matched experiences from within their organisations. Nevertheless, most partici-

pants perceived the attacker personas as very convincing and credible overall (also outside of their organisation): with almost 90% viewing them as "credible" (Q21; 89%; 57) and agreeing (51.6%, 33) or strongly agreeing (37.5%; 24) that "the personas could be real people and adversaries that actually exist" (Q20). Lastly, the practitioners showed a similarly high level of empathy for the attacker personas, with 85.9% (55) agreeing/strongly agreeing that they understood their motivations as portrayed in the profiles.

Relevance & applicability — The fourth construct focussed on how relevant and applicable in practice the attacker persona set was perceived by the practitioners, with 64 participants answering these questions (at least partly). As a positive outcome of the survey, nearly 60% of participants (58.7%; 37 out of 63 valid responses) agreed/strongly agreed that they had "learned something from reading through these profiles" (Q22), with 27.0% (17/63) undecided at this point. But while many practitioners perceived the method to be of practical value and applicable to their organisation and role (Q24), with 54.7% (35/64) agreeing/strongly agreeing to the related statement, a large number of participants were not sure about the exact value attacker personas could provide to them (31.3%; 20/64), with some dismissing the method ("I don't see practical value and applicability of this method to my organisation or job role"; strongly agree: 4.7% (3/64) and agree: 9.4% (6/64)). Similarly, participants would then either see potential in using attacker personas as a method in their role (53.1%; 34/64) or not (25.0%; 16/64), with 21.9% (14/64) not decided either way. This may also be related to a relatively large group of participants (33.9%; 21/62) criticising personas as too generic (Q13); with a further 32.3% (20/62) neither disagreeing or agreeing on this matter and only 33.9% (21/62) feeling confident that this was not a weakness of the attacker personas.

Usefulness & willingness — This last construct looked at the perceived usefulness of attacker personas as stated by practitioners, as well as their willingness to employ them in practice, with 62 participants scoring the statements in this construct. A large number of participants (77.4%; 48) agreed/strongly agreed that the attacker persona set from this thesis as shown to them could be "useful in understanding the potential adversary landscape to digital banking" (Q26). They were almost as supportive (66.2%; 41) for attacker personas in general as a "useful tool for speaking to senior stakeholders in my organisation" (Q27), although that meant that around one third of participants (neither disagree or agree/disagree/strongly disagree: 32.8%; 21) would likely not be prepared to use them in this way. Interestingly, support for using attacker personas "for training or raising security awareness in my organisation" (Q28) seemed stronger, with 83.9% (52) of participants agreeing on this (with 24.2% (15) of them agreeing strongly). Despite this, participants were not entirely sure whether using attacker personas based on their own data specific to their organisation would be useful to them, with only 56.4% (35) showing agreement (or strong agreement) to this statement (Q29), while more (67.7%; 42) thought tailored attacker personas may be useful to someone else in their organisation. In line with this, a considerable number of participants (disagree/strongly disagree: 32.2%; 20) would therefore "not be interested in taking part in an exercise to create attacker personas specific to my organisation or work" (Q31), with a further 29% (18) of participants undecided on this. Encouragingly, 38.7% (24) participants stated that they were interested (or very interested) in participating in such an exercise in the future.

Further input from practitioners — Given the opportunity to provide feedback outside of the statement questions, several participants used the chance to stress that they actually liked the personas, calling them e.g. "useful and relevant" and "well-designed" or simply stating "love the scenarios as it really brings it to life". Furthermore, a number of examples showed deeper engagement, strong interest and evidence of time spent with the attacker personas, e.g. with one participant joking about the personas: "if it wasn't for the criminal record, Bruno, the maths genius hacker who can't find a job, seems like a great hire". One participant also highlighted the personal learnings gained from reading through the attacker personas, while another one saw "great benefit in using them to educate colleagues that do not work in a security or fraud area and for operational staff new to fraud". Two comments were made on the personas representing "real-life characters" and feeling "real" — although this was directly contested by others.

The attacker personas were also strongly criticised, mostly for appearing generic and stereotypical to some: "I felt the persona of the Russian criminal mastermind felt rather clichéd and difficult to take seriously. The other personas felt more real" and "my only real issue is that the personas were quite stereotypical, largely white male [...] the criminal world is made up of all types of people so a little more consideration here would make it feel a bit more genuine." Another participant also could not see any value in the persona method for his work: "I do not see how this helps combat cyber security risk in digital financial services — it is what criminals do, how they do it, and how to stop it which is relevant — not what sort of people they are."

Lastly, while several participants seemed interested in using attacker personas in the future, a number of adaptations and improvements were suggested, e.g. to combine the attacker persona method with "known threats and target institutions as well as wider criminal organisations — without this it is generic" or to tailor the attacker personas further to financial services. Furthermore, a participant remarked that "if the personas included facts about [...] how the crime is committed, including empirical statistics — it is that which would be valuable information".

7.3.3 Further results: feedback for individual attacker personas

While some qualitative feedback from practitioners was aimed at the overall attacker persona set or attacker personas as a method in general, a selection of responses, also received during the initial pilot study of the survey as outlined in Section 3.5.3 on p.86 were very specific to individual attacker personas. An excerpt from these quotes is shown in Figure 7.11 and all feedback received is listed under the persona affected in Tables 7.2 to 7.4 (overleaf).

Similar to the iterative process used in Chapter 6 around attacker typologies (where validation results from heuristics and peer review were used to develop the latest iteration of the typology as included in this thesis), the feedback in Tables 7.2 to 7.4 has been used to refine the respective attacker personas towards the iteration included in this chapter. Where changes have been made, this is marked in the tables and also further commented in the discussion following this section. This is directly in line with the last step in Nielsen's 10-step process model as outlined in the research procedures in Section 3.5.3 p.86.

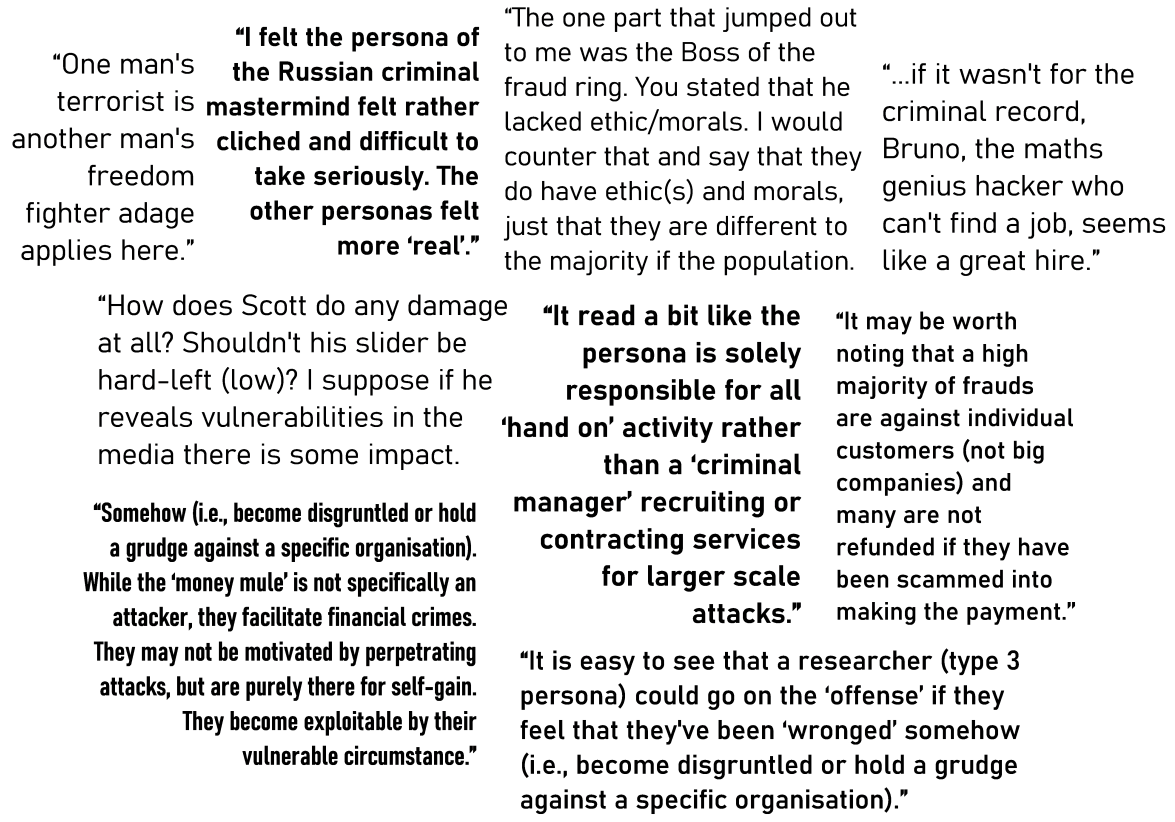


Figure 7.11: ***Selection of survey participant quotes: individual persona feedback***

Feedback	Stage	Action	Amendments	Previous version
"While the 'money mule' is not specifically an attacker, they facilitate financial crimes. They may not be motivated by perpetrating attacks, but are purely there for self-gain. They become exploitable by their vulnerable circumstance."	Survey	No		
"Banks actually share details of confirmed fraudsters and will essentially blacklist them, so other banks won't open accounts for them."	Pilot	Yes	Change made to narrative scenario (p.263): new (fake) identity required to open new bank account	Was likely factually incorrect: "even when Santander investigate and eventually close his account, he gets advice from his contact and manages to open another account with Barclays."
"It may be worth noting that a high majority of frauds are against individual customers (not big companies) and many are not refunded if they have been scammed into making the payment."	Pilot	Yes	Change made to narrative scenario (p.263): emphasis on persona's moral code — he may not see people as the victim. Added new section: "Banks have never meant a lot of good to him [...]"	

Table 7.2: ***Practitioner feedback for individual personas I: Kev, the money mule***

Feedback	Stage	Action	Amendments	Previous version
"It is easy to see that a researcher [...] could go on the 'offense' if they feel that they've been 'wronged' somehow (i.e. become disgruntled or hold a grudge against an organisation)."	Survey	No		
"How does Scott do any damage at all? Shouldn't his slider be hard-left (low)? I suppose if he reveals vulnerabilities in the media there is some impact."	Survey	No		

Table 7.3: ***Practitioner feedback for individual personas II: Scott, the security researcher***

Feedback	Stage	Action	Amendments	Previous version
"It read a bit like the persona is solely responsible for all 'hand on' activity rather than a 'criminal manager' recruiting or contracting services for larger scale attacks."	Pilot	Yes	Change made to persona profile (p.180): added 'team manager' aspect to persona profile	Was likely unrealistic: the focus was on the Bruno persona completing a lot of tasks himself rather than employing and managing others
"If it wasn't for the criminal record, Bruno, the maths genius hacker who can't find a job, seems like a great hire."	Survey	No		
"I felt the persona of the Russian criminal mastermind felt rather clichéd and difficult to take seriously. The other personas felt more real".	Survey	No		
"The one part that jumped out to me was the boss of the fraud ring. You stated that he lacked ethic/morals. I would counter that and say that they do have ethic(s) and morals, just that they are different to the majority if the population."	Survey	Yes	Change made to persona profile and narrative scenario (p.180 and p.253 respectively): changed wording in biography and added section on moral values	Was likely unrealistic: "He is a professional criminal through and through without morals or any ethics in his acts..."
"These guys are highly organised and motivated and commit fully with extreme prejudice in some scenarios. The returns are just too good and they want to maximise their investments."	Survey	No		

Table 7.4: ***Practitioner feedback for individual personas III: Bruno, the gang leader***

7.4 Discussion

This section reflects on the results of the attacker persona creation process as defined in the research procedures in Section 3.5.3 and documented in Section 7.2.2, considering both these outcomes as well as the evaluation results from the survey study undertaken in Section 7.3. Specifically, this section discusses positive aspects and benefits of attacker personas identified both in the creation process and the survey, followed by a note on perceived limitations and potential practical hindrances when working with attacker personas. Lastly, the continuous further development of the attacker persona set introduced in this thesis is discussed, together with a statement on potential starting points for future research efforts concerning attacker personas as a method in general.

7.4.1 Positive factors and perceived benefits

Positively reflecting and summarising on the attacker persona creation process and related evaluation results, the method and data sources relied on have produced an overall convincing and well received attacker persona set, scoring high levels in all persona perception constructs of the practitioner survey including perceived clarity, credibility, relevance and usefulness. This is particularly encouraging considering only 20% of survey participants stated that they had come across the concept of attacker personas or similar representations before, making attacker personas seem a readily understood and accessible concept to most reviewers, with many participants even regarding the attacker personas as enjoyable to read through. In addition to this overall positive tendency, further benefits could be identified directly from this chapter, both specific to the attacker persona set introduced and the method in general:

Relative efficiency and speed of iteration in attacker persona creation — firstly, the construction method based on Nielsen [29][30] as proposed in the research procedures in Section 3.5.3 and subsequently carried out to arrive at the iteration of the attacker personas as included in this chapter, has enabled the creation of an attacker persona set based on secondary data in a structured and efficient manner. Additionally, an initial iteration and feedback cycle has already been carried out and included in this chapter, with this current iteration of the attacker persona set awaiting further review and change cycles. While further practical application of Nielsen's method in the context of attacker personas are indicated, this initial work offers some positive evidence on the suitability of the method and a potential reference point for other researchers.

Attacker personas as communication tools — with limitations, a significant proportion of practitioners stated that attacker personas had the potential to be useful communication tools (somewhere) in their organisation: approximately two thirds agreed/strongly agreed that they could be a "useful tool for speaking to senior stakeholders" or saw them as "useful to someone else in their organisation". This is in line with suggestions on the purpose of conventional user personas in previous literature and key textbooks (e.g. Adlin & Pruitt [28] ch.5 or Nielsen [30] ch.8). Beyond communicating with attacker persona sets at an advanced stage of their development, even 'imperfect' early persona drafts seemed to encourage informal discussion and feedback. In the case of

this research, the intranet discussion board in the participating organisation was used, and several participants exchanged their views with the researcher via email (e.g. in relation to the changes to the attacker personas as suggested in Section 7.3.3).

Attacker personas for training and security awareness — support for using attacker personas within the context of security training programmes seemed relatively strong in the survey sample (nearly one quarter in strong agreement; with over 80% of all participants agreeing on this and qualitative feedback also referring to this). While the usage of 'negative' personas like attacker personas and their usage within security awareness programmes seems limited at this point in time, user personas have been examined in more detail in this context, with e.g. Lewis & Coles-Kemp introducing comic strips and engaging storytelling as an option to extend on traditional personas, also in the context of awareness in [378]; and more specifically Ki-Aries et al. [167] who introduce an iterative 'persona-centred' methodology for security awareness programmes — insights from these works may be drawn upon for establishing the potential of attacker personas in a security awareness context.

Engagement and empathy with the attacker personas — in line with previous research (e.g. Grudin [379] or Bødker et al. [41]), practitioners reviewing the attacker personas showed a relatively high level of engagement and empathy throughout the process, commenting on (also critically) individual personas or narrative scenarios. While the survey in this research was used primarily as a remote evaluation tool in this thesis, this indication is promising for further collaborative real-world efforts around attacker personas, showing the potential of attacker personas as a method that may actively engage practitioners — in this context, almost 40% of survey participants seemed willing to participate in a future collaborative exercise around building an attacker persona set.

7.4.2 Limitations and practical hindrances

While the attacker personas were mostly received positively and the underlying construction method seemed to provide adequate structure to build them efficiently and effectively as discussed in the last section, a number of problematic areas can be noted on completion of this iteration of the persona set. Initially, two methodological constraints can be named which have already been pre-positioned for this work: firstly, the survey sample size is relatively small (N=85) for the overall population of financial services professionals with an interest in security or related topics — this has been defended in the research procedures in Section 3.5.3 p.87, accepting this size in a foundation study context. Secondly, potential survey bias was raised in the research procedures. However, on reflection, no noticeable levels of either central tendency bias (with extreme response categories such as strongly agree/disagree used throughout by the participants) or acquiescence bias (with participants not just agreeing, but also disagreeing for reversely phrased question) were detected. Furthermore, no evidence of social desirability bias was evident (no participants aimed to present themselves or their organisation more positively), while response bias had already been tested for and generally ruled out in Section 3.5.3 p.87 — in summary, no significant bias skewing the survey results had to be considered during their interpretation.

Beyond this methodological considerations, the following limitations and practical issues can be identified for this study:

Challenges and difficulties around persona design — practically designing the attacker personas proved challenging in parts, for example in choosing adequate profile pictures: while stock images were carefully selected and licensed by the researcher, 60% of survey participants were not entirely convinced by them. This is in line with previous research on imagery as used with conventional personas [380], highlighting the impact that photography choice may have on the perception of the personas amongst the stakeholder group. Here, early collaboration and testing around photography choice to be used may help to counter negative effects and bias. Another issue was the level of detail available from the original data sources to build the attacker personas. As the attacker personas were built on secondary data from case reports and articles over primary data from interviews with digital banking attackers and other cybercriminals, this data was often focused on facts around the case (for example modus operandi or monetary damage inflicted) rather than personal information about the attacker or their emotions. To overcome this issue, additional sources were added to expand on specific characteristics of attackers, round off the persona profile and make the personas more realistic, easier to understand, accept and relate to for stakeholders (see Section 3.4.3).

Potential lack of clarity around practical value of the method — a relatively large group of survey participants (near 50%) did not see explicit value or applicability of attacker personas to their role and were therefore not likely to use attacker personas in practice. Additionally, questions concerning tailoring or further extension of attacker personas resulted in potentially unreliable scores eliminated from the interpretation due to low Cronbach's alpha scores. Both of these aspects may indicate an inadequate understanding of the method, but also a lack of clarity on the value and benefit it may provide — this may be attributed to the usage of a survey-type study outside of a specific work environment rather than employing a dedicated, collaborative buy-in approach in an organisational or team setting as demanded by Nielsen [29][30] in her 10-step process model. Furthermore, many participants did not have experience with either personas (over 50% has not come across or worked with personas before) or attacker personas (80%) — these results may indicate that further detailed introduction and explanation of the persona method may be required in practice. Additionally, further enquiry into the integration of attacker personas into everyday work routines including security assessments and risk scenarios would be of interest. Therefore, personas are one of the discussion topics included when talking to financial services practitioners in Chapter 8.

Potential stereotyping in attacker personas — some participants perceived the attacker personas as "clichéd" or as stereotypes, with one practitioner stating that: "(my) only real concern is it's all a bit stereotypical (largely white male). A bit more diversity would help it to feel more genuine". This issue has been identified in user-centric research on personas before (e.g. Turner & Turner [162] or Grudin [379]), with suggestions to carefully review before moving onto either acceptance or amendments. In the context of this thesis, it was decided to not change the attacker persona set significantly at this point as the structure, selection of individual attacker personas and profiles were

largely determined by the underlying real-world data as defined in the research procedures. However, this issue will at least require further enquiry or testing (potentially using an A/B test, where two different attacker personas sets are tested for their performance with the target audience) if not changes to the attacker persona profiles in future (see Section 7.4.3).

Not highly specific in a real-life organisational context — lastly, it is important to realise that the attacker personas introduced in this work remain to a certain extent generic. And they will likely continue to do so unless they are placed in a very specific organisational setting with its own data and research, but also people, their knowledge, experience and work routines. But this level of specific attacker definitions and applicable narrative stories paired with the reflection of organisational culture, knowledge and skills may exactly what is needed to make (attacker) personas work most effectively in practice (see also Nielsen's process model step 9, p.85; also in Pruitt & Adlin [28] ch.5). In this context, future publications detailing examples of organisation-specific attacker persona sets, their practical usage and also construction process coming directly from industry would be of significant benefit.

7.4.3 Continuous development and future work

When following Nielsen's process model through all 10 steps from start to finish, continuous development stands at the very end: this tests whether the attacker personas are still valid, work for all stakeholders and still represent the current threat landscape and related attackers. For this purpose, Nielsen [29][30] recommends usability tests with the users of the personas as well as gathering their feedback on an ongoing basis. A starting point for this iterative approach has been implemented within this thesis, with Section 7.3.3 describing practitioner feedback and changes made to earlier versions of the attacker personas where applicable — this has produced the second iteration of the attacker personas as included in Section 7.2.2 and Appendix A, which is now ready for practical everyday use as well as subsequent iterations based on further rounds of practitioner feedback. Here, Nielsen [29][30] suggests annual review intervals — this seems appropriate to balance the effort of re-designing the personas and the ongoing need to reflect the current threat landscape. Furthermore, with future developments and trends in cybercrime expected to change the overall attacker landscape, the underlying data input into the attacker personas (data sources as described in Section 3.4) will likely require updating and extending over time to help keep the attacker persona set as current, realistic and relevant as possible.

Further to the regular, continuous development of the attacker personas, subsequent iterations of the attacker persona set should also aim to address two of the issues identified through the evaluation and feedback loop within this thesis:

Overcoming stereotypes — user-centric design literature offers ample perspectives on addressing this issue (e.g. [29][30][162][379]), avoiding or accepting stereotyping where required. Ultimately however, the level of validation and buy-in shown by stakeholders for the personas created (refer to step 7 in the process model, p.84) defines their initial acceptance and successful long-term usage within an organisation. Ideally, this is

achieved by collaborating directly with all stakeholders of the persona set throughout the creation process, refining persona characters and profiles where necessary to create convincing and realistic representation. This could also include further review rounds of specific attacker persona details, e.g. profile pictures.

Moving from generic to specific — for the attacker personas to provide true benefit, they need to be very specific to an individual organisation and use case — very likely more specific than introduced in Section 7.2.2. This was evident in the survey, where around two-third of participants either considered the personas as generic or did not disagree to them being generic — this was supported by qualitative statements from several respondents as well (from Section 7.3.3). To address this issue directly, subsequent attacker persona sets could for example be tailored to specific small-scale scenarios, e.g. the design of user access rights for a content management system in a bank or new mobile banking functionality. Where available, research data specific to individual organisations could be used to refine future attacker persona sets.

Beyond the future development of the specific attacker persona set introduced in this thesis, but based on the learnings and limitations raised in this work, the following aspects may serve as starting points for future research efforts on attacker personas in general:

Methodological refinement and advancement — extending on this work, more practical examples for building attacker personas following the entire process model from early stages to persona maturity are required, both for the case of digital banking and for other industries. It is hoped that this will help to develop methodological approaches further, in order to shape the best practices for attacker persona creation in line with the robustness of user-centric approaches. As mentioned, the area of security awareness could form a particular focus for future research in this context.

Improvement of data sources — one of the largest difficulties in building attacker personas is the lack of access to high quality data source materials containing enough depth and detail to form meaningful and realistic attacker personas. This thesis has taken an alternative approach by using publicly available sources to produce relatively generic attacker personas. For any organisation interested in the attacker persona concept however, some preparation where potential attacker data is collected continuously (even in a fairly informal way) may be of benefit and ultimately lead to better, more relevant attacker personas.

Integrating the attacker persona method into the overall risk model — another question about attacker personas is their place within the overall security assessment and risk modelling ecosystem of an organisation. This certainly also relates to the question of what benefit the usage of attacker personas is to organisations. As highlighted in the background of this thesis in Section 2.2, using attacker-centric approaches to threat modelling is not without drawbacks and attacker personas are unlikely to provide a stand-alone risk assessment tool. To address this, organisations need to make sure that they are clear how attacker personas are going to be used from the start and how they complement other assessment and modelling methods. It also needs to be clear how the 'finished' attacker personas will be transitioned into everyday usage by stakeholders

to get the most value out of them. Attacker personas in daily work routines are also touched on in the next chapter, where attacker-centric thinking and work practices are discussed with financial services professionals.

7.5 Conclusion

Reflecting on the tangible deliverables of this chapter, a complete attacker persona set specific to digital banking has been successfully created, with the practitioner evaluation undertaken in the context of the study confirming an overall positive perception of attacker personas created: most participants perceived them as convincing, credible and realistic. Nielsen's 10-step process model as a construction method therefore seems suitable to be adapted for a security context to support the creation of attacker personas, while secondary data may also serve as a valid input for such personas as demonstrated in this study.

These results can also be viewed as a detailed showcase and fully working example of attacker personas as an attacker-centric method in security, with uses to practitioners and organisations potentially interested in adapting the method, but also designers and developers looking to build their own attacker personas. Additionally, this work can be seen to directly supplement previous academic research introducing and focussing on attacker personas as a method (e.g. [7][27][44][120]) — here, authors of future works in this area could reference this full attacker persona set in addition to their own abbreviated persona examples, saving their time and effort while ensuring full focus on their research topic.

Outside of this work specifically, there have been some indicators for general attacker persona usage in this study, as well as some emerging problem fields. Attacker personas seem to be well suited for communication purposes, either when speaking with senior, but potentially non-technical stakeholders or as part of security awareness programmes. Additionally, their visual and accessible nature seemed to invoke empathy and foster active engagement in the reviewers, hinting at their potential for making ideal tools to enable communication and collaboration in organisations. Equally however, several problems around attacker personas remain unsolved in this study: while the process of persona creation including the danger of stereotyping continues to be challenging (but can be addressed by making careful design decisions), difficult questions around the practical value and meaningful, efficient integration into current work routines remain for attacker personas.

While not specifically aimed at attacker personas, the next chapter seeks to enquire into the state of attacker-centric security and thinking in a practical context through conversations with a number of senior financial services practitioners around this topic — attacker personas as an attacker-centric tool also find inclusion in these discussions in Chapter 8.

"(Attackers) are a little bit detached from me — I am not necessarily happy about this"

— Fraud strategy manager
in financial services;
interview excerpt, 2019

8

Attacker-Centric Thinking in Security

This chapter examines the position of attacker-centric thinking and approaches in security, opening out the scope of discussion at the end of this thesis by moving beyond specific approaches towards a more holistic view provided by practitioners. 12 in-depth interviews with senior financial services professionals working in the areas of security, fraud and risk are carried out and analysed using thematic analysis as defined in the research procedures. Building on the literature review of related materials presented in the background section, results are summarised and transformed into a list of recommendations and guidance around the effective usage of attacker-centric approaches.

Most of this thesis has been dedicated to the humans behind attacks and cybercrimes, whether in the large analysis of attacker characteristics and behaviours, the extension of attacker typologies to digital banking or the visualisation through attacker personas. These efforts have yielded interesting results, with several recommendations for their further usage made so far (e.g. attacker personas to support security awareness; in Chapter 7). And these results don't exist in isolation — they have been precedented by similar research in the past, like the works on attacker categorisations by Hald & Pedersen [24], Seebruck [25] or De Bruijne et al. [26] or attacker personas in Atzeni et al. [7], Faily & Fléchais [27] or earlier Steele & Jia [44].

The background section of this thesis has introduced the notion of 'attacker-centric' ap-

proaches to security, also discussing threat modelling with an attacker focus — in this context, Shostack ([6] ch.2) for example observes limitations to attacker-centric approaches citing potential lack of structure and rigour to model against as a hindrance and recommending asset-based, software-/system-based or threat-/risk-based strategies as an alternative (also supported by e.g. UcedaVélez [381] or Mirembe et al. [75]; as discussed in further detail in Section 2.2). Given these theoretical concerns, but also considering the variety of attacker-centric methods in existence (such as typologies or personas), how do practitioners view and use formal or informal attacker focus in their daily routines — do they share these concerns? What attacker-centric methods and tools do they use in their practice? And how do they see the potential future of such approaches?

Similarly, as part of the evaluation efforts for attacker personas in Chapter 7, the perception of this particular attacker-centric tool by financial services professionals has been examined, using a survey-type questionnaire. Extending this focus to security in general (rather than attackers personas specifically) and in answer to the research questions posed in Chapter 1, this chapter seeks answers to how financial services practitioners in real-life settings think about attackers and use attacker-centric approaches in their daily work routines. To enable this, 12 semi-structured, in-depth interviews with senior financial services professionals in security, risk and fraud as a corporate elite (as defined in Section 3.5.4) were carried out and analysed using thematic analysis (refer to the related research procedures in Section 3.5.4).

Based on these research procedures in Section 3.5.4 and the theoretical background on the topic presented in Section 2.1, this chapter is structured as follows, based on the research questions set out in Section 1.4. Firstly, the results from the interviews are summarised around six thematic areas: threat intelligence as a basis for taking an attacker focus, intended purpose and gains, practical considerations, integration with the wider digital banking business environment, future directions and perceived limitations (refer to Table 8.1 overleaf). This is followed by a brief reflection on the interviews by the researcher, before moving into a discussion containing two parts: firstly, a comparison of these practical insights with previous literature is drawn, including a segmentation of types of attacker-centric thinking encountered in both theory and practice. Secondly, derived from the findings, a 12 points list of recommendations and guidance on how to use attacker-centric approaches most effectively is presented. Lastly, a conclusion and reflection on how these insights relate to earlier chapters is provided.

8.1 Results

Based on the thematic analysis carried out and directly reflecting the coding structure in NVivo as a supporting software tool as defined in the research procedures in Section 3.5.4, this section structures the central insights gained from the interviews around six key themes and their subordinate content (refer to Table 8.1 overleaf). Figure 8.1 on p.205 provides an indication of the nature of data collected, showing a selection of practitioner quotes. Initially, the relative importance of threat intelligence (including attacker-related information) as an underlying enabler for attacker-centric thinking and employing an attacker focus is highlighted, followed by insights on the perceived value and overall purpose of such an approach

Threat intelligence as the basis for an attacker focus	Building a comprehensive picture of the threat landscape
	Information gathering, sharing and reassurance
	Open source information: defenders vs. attackers
Purpose and gains of an attacker focus	Supporting a strategic view
	Understanding the criminal business model
Practical considerations for attacker-centric methods	Attacker modelling in practice: view of existing groups
	Attacker modelling in practice: threat libraries, scenarios and attack path maps
	Representations of the human attacker
	Attacker determination as a new profiling dimension
Integrating attacker-centric aspects in a digital banking business environment	Work routines and attacker focus
	Balancing business, customer and security needs
	Mapping and securing the digital customer journey (online and offline)
Future directions for attacker-centric security	Data-driven attacker modelling
	Emerging technologies as a risk and opportunity
	Increasingly complex and interconnected systems
	Threat readiness and proactive attitude
Perceived limitations	

Table 8.1: ***Overview of interview study key themes and subthemes***

as provided by the participants (in Sections 8.1.1 and 8.1.2). This is followed by practical ways of integrating attacker-centric thinking and related methods in a digital banking business context (Sections 8.1.3 and 8.1.4) as outlined by the interview participants. In alignment with the discussion topic on the future potential of attacker-centric methods in security posed to the participants, Section 8.1.5 documents such expectations for the future. Section 8.1.6 closes this results section with the presentation of perceived limitations and hindrances to adapting an attacker focus as told by the participating banking practitioners.

8.1.1 Threat intelligence as the basis for an attacker focus

Building a comprehensive picture of the threat landscape — threat intelligence, which can be defined as "the output of analysis based on identification, collection, and enrichment of relevant data and information" to inform security decision-making [382], is viewed as paramount for understanding and modelling threats against an organisation — this also includes intelligence on attackers. The interviewed practitioners were aware of or actively using a number of threat intelligence approaches and resulting data insights, mentioning e.g. initiatives to source contextual attacker data to trace actors on the darknet via research and intelligence suppliers, but also more generic attacker profiling efforts referring to e.g. attack methods and tools or demographic factors including the geographic origin of attacks. In this context however, limitations were described as to

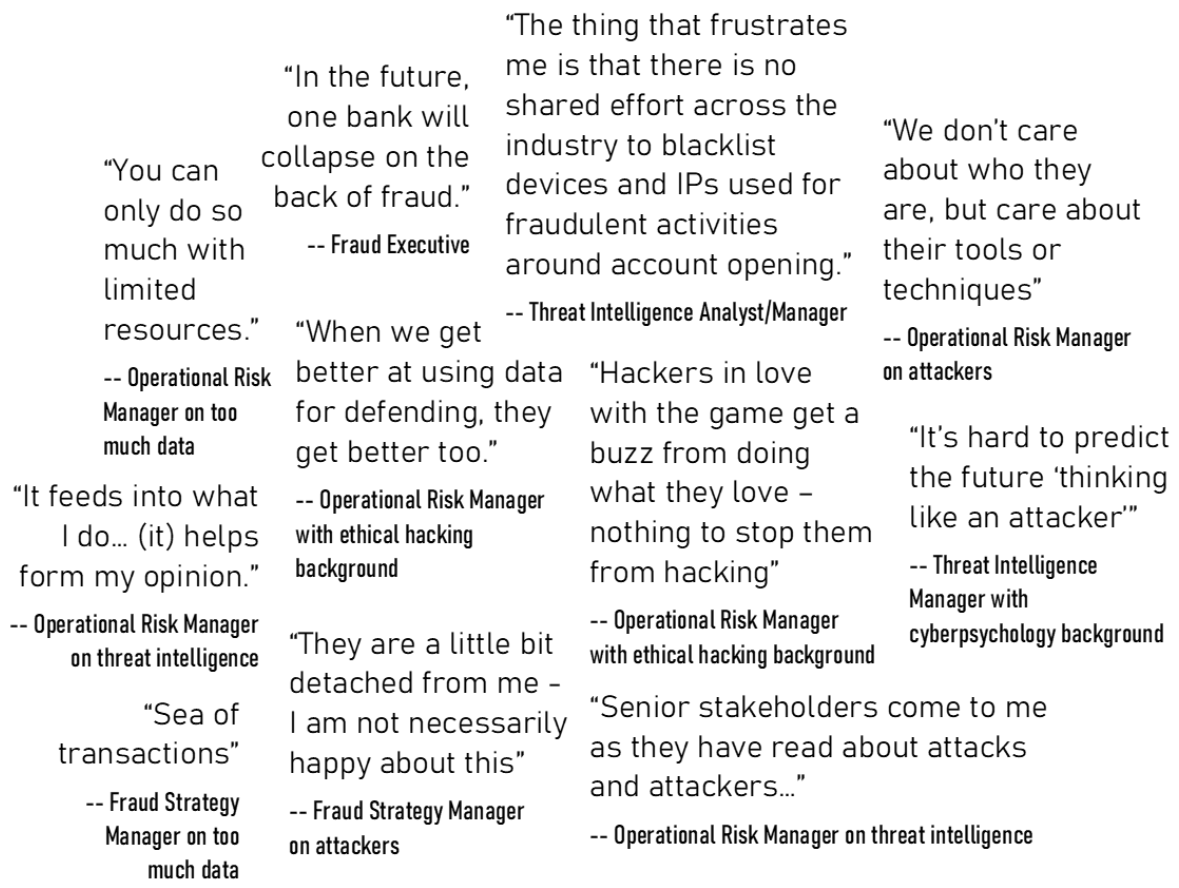


Figure 8.1: ***Selection of interview participant quotes***

what data and information banks could source for their threat intelligence programmes (see note on limitations). Furthermore, the right organisational setup regarding threat intelligence mattered to one participant: in banking, many attacks and crimes cross the line between the cyber and physical world (e.g. ATM related crimes). In his opinion, it therefore makes sense to move from having separate teams each with separate intelligence teams to an aligned intelligence team spanning physical and cyber security, including ATM and mobile security (threat modelling senior manager).

Information gathering, sharing and reassurance — threat intelligence also plays a key part in informing (and reassuring) senior stakeholders about current threats, as for example told by an operational risk manager: "senior stakeholders come to me as they have read about attacks and attackers [...]". Other security, risk and fraud teams across the organisation will heavily depend on threat intelligence teams and their analysis as a way of thinking about attackers in their everyday roles, e.g. through threat radars and assessments (as mentioned by a threat intelligence manager).

Open source information: defenders vs. attackers — while open source information (e.g. social media networks such as Twitter) is an extremely important intelligence source for defenders, the same logic applies for attackers: they will also be using open source intelligence, for example to find out about new attack surfaces into banks or their suppliers. This 'arms race' between these two groups was discussed in detail by one of the risk managers with an ethical hacking background: "when we get better at using

data for defending, they get better too". Open source information may also have a far more direct attacker focus: one participant mentioned the possibility of identifying vague direct threats against the banking organisation through open source monitoring (e.g. a planned attack could be announced or arranged by an individual on social media). Similarly, media impact and reporting on (potential) attacks and attackers was also seen as a key aspect to be monitored by one of the security executives.

8.1.2 Purpose of and gains from an attacker focus

Supporting a strategic view — in terms of benefits gained from an attacker-centric perspective, an attacker focus was seen as more helpful for a "tactical level security perspective" (fraud senior manager) or "broad and shallow macro-level strategic view" (operational risk manager) rather than modelling threats directly on attackers. The threat modelling senior manager and security strategist in the participant group stated "there is a tendency to look at things at a very granular level rather than from a strategic point of view", preferring a strategic view as a proactice approach to identify and assess potential future threats. Furthermore, using exemplary attacker group representations was seen as beneficial for taking a "proactive approach to identify and assess potential future threats". These statements are certainly related to the criticism exercised against attacker-centric modelling by Shostack ([6] p.40) — while using attacker information or representations to model specific threats and attack techniques might not work very well, using such information for taking a more strategic, long-term view may be a more efficient starting point. This assumption seemed generally supported in the sample, e.g. by a threat intelligence manager: "it's hard to predict the future thinking like an attacker" or by an operational risk manager: "we don't care about who they are, but care about their tools/techniques". Another strategic aspect around 'knowing your enemy' is also mentioned: rather than informing exact countermeasures and mitigations to be used, the nature of the expected attacker (group) behind an attack may define the strategic defence approach, i.e. organisations under attack could decide to focus on 'damage limitation' only if up against powerful nation state attacks (as told by the security executive) and also by a threat intelligence manager: "knowing who is behind the attacks may help to understand how far they will go". This is likely to refer to organisations focussing their efforts to maintain or restore minimum services during or after an attack (and communicate the chosen approach appropriately to the public, as mentioned by an operational risk manager) rather than trying to fully return to the pre-attack state too quickly, given the almost infinite attack power expected from nation state attackers.

Understanding the criminal business model — gathering and analysing attacker information was largely seen as helpful in understanding the business model of organised groups, supporting a holistic view of the overall security ecosystem, "making sense of what's happening" (threat intelligence manager). Specifically, "understanding people" is seen "as likely to mean a better understanding of cyber operations" and business models (as told by a threat intelligence manager). The attribution of the globally devastating WannaCry ransomware attacks to North Korean state-sponsored hackers was used as

an example to illustrate this: explaining WannaCry as an attack from a nation state actor rather than an independent group "made sense" to them (due to the large scale of the attack and the previously unclear motivation behind it). It was also seen as helpful for future modelling purposes, where such group examples could then be included, e.g. in threat scenarios.

Similarly, understanding further business model elements such as 'hackers for hire' was mentioned in this context by a security executive, with a senior manager distinguishing between 'hands-on' attackers and 'criminal managers' recruiting or contracting services for large scale attacks (explicitly mentioning the NCSC report on understanding the online business model behind cybercrime [235]). Here, the complexity of criminal business models was further hinted at: hackers for hire may be recruited (or malware may be purchased or commissioned as mentioned by a threat intelligence manager) by different criminal groups — meaning that the same attack patterns and signatures may be present across various groups and attacks. Overall, participants talk confidently about the business model employed by attackers, e.g. a senior fraud manager speaking of "massive organised criminality with call centre-scale type operations: huge, organised, sophisticated and successful at scale", "trying to run a business just like we are".

8.1.3 Practical considerations for attacker-centric methods

Attacker modelling in practice: view of existing groups — considering attacker groups and relationships seems to form an important element in modelling attackers in the organisation, as evidenced by two participants talking about this aspect. Group information is seen as more relevant than information on single attackers: "(threat intelligence) doesn't usually go down to the individual, but group levels" (threat intelligence manager). This is supported by a threat intelligence senior manager describing threat scenarios often modelling attackers on past experiences or incidents as well as existing groups, employing a neutral label rather than an exact group name. As an example of an existing group used as a blueprint for practical modelling, Lazarus is mentioned in the interview: as investigated and presented in detail by Kaspersky Lab [383], the Lazarus group is believed to be behind one of the largest cyber heists against a financial institution to date, managing to transfer 81 million US dollars from the Central Bank of Bangladesh. Kaspersky describes Lazarus as "a notorious cyber espionage and sabotage group responsible for a series of regular and devastating attacks, and known for attacking manufacturing companies, media and financial institutions in at least 18 countries around the world since 2009" — this hints at the level of danger and the sort of attacker groups banks are looking to protect themselves against.

Attacker modelling in practice: threat libraries, scenarios and attack path maps — a number of approaches including attacker-centric aspects are mentioned by the practitioners in the sample. A threat intelligence manager describes working with a customised cyber threat list created through collaborative industry efforts, but also the usage of existing databases and libraries such as the MITRE Common Vulnerabilities and Exposures (CVE) list [384]. Threat scenarios are mentioned (albeit without specific procedural

detail): "thinking through a scenario from an attacker's perspective and trying out what they could do" (threat intelligence senior manager). This is in line with existing approaches in the banking sector — Green for example introduces a structured approach to 'cyber scenario planning' based on threat actors and impact analysis for a number of scenarios [385]. Three of the participants also describe the importance of mapping the attack path, considering potential or previously observed entry points exploited by attackers at either an individual user or at an organisational level — industry-wide efforts may also support this through sharing such maps and experiences, e.g. at which layer of defence the attack was ultimately stopped (as told by a threat intelligence manager). Lastly, the cyber kill chain model (as defined earlier in this thesis on p.28) as an approach with a strong attacker focus is mentioned by a security executive, based on a number of generic attacker categories defined by modus operandi, capabilities and motivations which are aligned to the seven phases of the attack kill chain (reconnaissance, weaponisation, delivery, exploitation, installation, command & control, actions on objectives).

Representations of the human attacker — an interest in attacker profiling including demographics like geographic location or nationality is displayed by several interview participants, with a number also referring to specific groups, similar to an attacker typology provided in Chapter 6: "I am aware of different attacker profiles such as internal fraudsters, members of a gang, [...]" (fraud strategy manager) or "distinct attacker groups are used, e.g. political/ideological, organised crime, [...]" (security executive). Additionally, a fraud senior manager explains the classification or attackers involved in banking fraud, with a distinction between third-party fraudsters[53], first-party fraudsters[54] and money mules (compliant/non-compliant). Four of the participants also mention the concept of attacker personas as examined in Chapter 7, e.g. "human representations such as personas may help to serve as a baseline and help to design against a large group of people/fraudsters, understand them better and visualise the knowledge we already have" (fraud strategy manager) or specifically for the case of money mules: "money mule data, risk profiles and demographics are known... usage of datapoints/analytics to identify money mules and fraudulent accounts can help to create 'persona' profiles" (security executive). Human attacker profiles are also viewed as beneficial for practical aspects such as security awareness or to train staff (operational risk manager) or to compare patterns of malicious attacker and genuine customer behaviour in fraud prevention (fraud senior manager). Lastly, one participant (security executive) also mentions support for victims as crucial, based on "cybercriminals harming people, not just banks".

Attacker determination as a new profiling dimension — another valuable insight resulting from an attacker-centric approach is attacker determination, as mentioned in two of the

[53]The Open Risk Manual defines this terms as: "third-party fraud means a fraud that is committed by means of use of a person's identity, such as the use of false identification documents, without the knowledge of the person whose identity is used to commit the fraud." [386]

[54]The Open Risk Manual defines this terms as: "first-party fraud means a fraud that is committed by an individual or group of individuals on their own account with no intention of any repayment of the loss caused." [387]

interviews (security executive and threat intelligence manager). While motivation of the attackers is considered in most attacker categorisations (as discussed in Chapter 6), determination is not mentioned specifically. But according to the interviews, the level of determination in the attacker, as well as the nature of motivation, is seen as important for defence. Knowing who is behind attacks is seen to help understand how far they will go, with for example nation state actors and other 'officials' as attackers likely to behave differently to professional criminals — this level of risk taking and behaviour could be explained by them being in probably less danger of being prosecuted in combination with an assumed high level of available resources.

8.1.4 Integrating attacker-centric aspects with the business environment

Work routines and attacker focus — most participants acknowledge the presence of some level of attacker-centric thinking, methods or techniques in their everyday work: attackers may play a role in job routines e.g. "as part of threat radars and assessments" (threat intelligence manager) or when working with tools, e.g. for fraud analysis and monitoring. Two of the participants also mentioned the problem of "too much data" in this context, making analysis at an individual attacker level difficult (see also Section 8.1.6). When describing their roles, most participants talked about the importance of collaboration to distribute attacker information across different functions of the organisation, e.g. through providing threat intelligence data, helping business areas through providing consultancy or by creating a proactive, "generative" risk culture to be "channeled into risk teams and the wider bank" (operational risk senior manager). As already indicated, attacker information may support such a collaborative culture, e.g. by helping to raise security awareness or to train staff (as told by an operational risk manager). However, a fraud strategy manager also made clear that he 'realistically had no time to think about attackers/adversaries on an everyday basis in his role' and that attackers therefore felt "a little bit detached to me — I am not necessarily happy about this". In direct relation, he and another participant (threat intelligence manager) emphasised the importance of "time to think (and not necessarily as a brainstorm/group thinking exercise)" and to "slow down" to "make things better" and "accommodate security and balance customers' needs/wants/expectations". A fraud strategy manager also stressed that the skills, experiences and knowledge in relation to attackers, are difficult to record and retain in modern workplaces undergoing constant change (including staff movements).

Balancing business, customer and security needs — attacker information naturally only forms a small part of everyday routines and tasks of the digital banking practitioners interviewed. After all, they are balancing a number of perspectives and stakeholders, focussing on business needs and meeting regulatory requirements. While security solutions, mitigations and the plugging of control gaps and their impact need to be costed up internally (security executive), external factors such as regulatory developments but also the competitive landscape (a senior fraud manager mentions the example of "recent industry developments which may have an impact on customers, e.g. the latest 'fraud guarantee' initiative from a competitor") make this a complex environment to

operate in and apply attacker-centric security principles to. On balancing risk and security with business requirements and customer needs, a risk senior manager views "cybercrime and cyberwarfare as a continuous and growing risk also for banks — this and rising customer expectations (better/faster) need competent people and the right controls". He underlines this customer focus taken by the organisation by describing a "fix-and-learn-approach" (fix it for the customer first and conduct a post-review) as part of an ongoing and iterative review of security controls.

Mapping and securing the digital customer journey (online and offline) — the concept of the digital customer journey and its relation to attackers is discussed by almost all participants: it signifies the path users and potential customers take to move through service and product sequences offered via the bank's digital channels including online and mobile banking. An operational risk manager working in technology explains that a "further move towards a 'digital bank' means external threats become more important... so further understanding of attackers would be useful". To accommodate this, "threat modelling of the customer journey at a transactional level (end-to-end including user registration)" is described by a fraud senior manager, and a threat intelligence manager has worked with "fraud process end-to-end mapping" where various user and attacker types (or personas) can be inserted into the sequence ('follow the money').

As individual elements of the journey may deter or encourage fraudsters, e.g. the login element or registration and account opening processes, they need to be analysed in detail, including related user behaviour, e.g. push notifications fatigue (as told by a fraud senior manager and security executive). Changes and new innovation to the customer journey may have a 'knock-on effect on fraud', therefore requiring risk assessments of the new functionality and "a look across the entire digital ecosystem as a potential fraud aggregator" — this is "in contrast to a generic model to explain fraud occurrences, but specific to customer journeys" with the aim to 'build security in' (as told by two fraud senior managers). Potential and previously encountered entry points of attackers can be mapped against the digital banking ecosystem and specific customer journeys, also considering non-digital, traditional elements like branches as vulnerabilities (e.g. for opening new mule accounts as mentioned by a security executive). However, a threat intelligence manager is critical of this approach in the future as "the question around which entry route an attacker could use becomes non-feasible/obsolete with increase in large, complex and interconnected technologies" (and the related difficulty to accurately and completely map the related customer journey). Lastly, one participant raises the point that "weaknesses and weak targets" along the digital journey are the same for all banks, including new entrants to the digital banking ecosystem (here, a security executive specifically mentions current UK challenger banks).

8.1.5 Future directions for attacker-centric security

Data-driven attacker modelling — practitioners in the sample generally expect attacker information to play a role in their future work, but with a strong focus on data patterns rather than informal human attacker descriptions. "Because ultimately, defining and

making these exact attacker profiles useful is so difficult" — the overall expectation for a fraud senior manager is to see more data-driven initiatives which may also include attacker information, e.g. data tracking digital footprints of devices or other biometric information for profiling. Several participants mention ML as a future opportunity to watch in this field, e.g. "data has always been in the focus to understand and prevent fraud and cybercrime patterns, but it will get even better (for example through ML to build fraud profiles)" (fraud senior manager). A security executive also recognises the potential to detect money mules and related patterns with the help of machine learning. At a more generic level, a (not further defined) "development towards scientific modelling for cyber risk" is expected by an operational risk manager in this context.

Emerging technologies as a risk and opportunity — in contrast to the last point, ML and AI is seen as a potential attack vector in the future: "another potential risk lies in the area of ML/AI: if this is not truly understood, unintended circumstances may arise from this. There is a risk for 'machine bias' and 'bots getting too clever'. Further difficulties in this area may be the difficulty to prove to the regulator what underlies decision-making. Lastly, there is the opportunity for manipulation (unintended or malicious)" (as told by a risk senior manager). Attacker-centric views are seen to likely play a role in designing new controls around emerging threats and changing the threat landscape, and to understand new security economics by an operational risk manager in the sample. Not directly related to attackers, participants mention other aspects on their professional 'roadmap' for the near future, e.g. secure customer authentication or regulatory requirements. A threat intelligence manager explicitly highlights future thinking around attacks against IoT and home devices or blockchain applications already presented in theoretical academic literature, but in his opinion requiring further definition of specific business cases and scalability. Lastly, data sharing between banks and other companies is viewed as a new opportunity (e.g. insights and business opportunities) and challenge (e.g. privacy, data protection and customer expectations that can't be met), with a risk senior manager citing the example of an UK challenger bank offering the switching of energy suppliers in-app to their customers.

Increasingly complex and interconnected systems — the digital banking environment of the future is complex, with pressures added by competitors, regulators, customers as well as technology and security requirements to be met: "it's only going to get harder to understand and will become more complex the more interconnected systems get. There are a number of significant influences such as cultural, technological, customer needs and wants or fraud risk. Examples would include third party systems such as Apple/Google Pay having an impact on internal processes or timelines" (as told by a fraud strategy manager). As already indicated, this also influences the potential value of attacker profiling and attack path mapping in the opinion of a threat intelligence manager: "the question around which entry route an attacker could use becomes non-feasible/obsolete with the increase in large, complex and interconnected technologies".

Threat readiness and proactive attitude — the question on using attacker-centric approaches in the future yields limited insights, but attacker information is seen to play a role going forward in threat readiness. Threat readiness as a discipline can be explained as

looking into 'unlikely' threats and establishing probable mitigations and solutions for them. This is roughly in line with the security-centric approach defined by the threat modelling working group at the OWASP summit [388], where every possible threat to the system is investigated. In regard to future threats, potential data breaches are identified as something to analyse further (as mentioned by a threat intelligence senior manager) — here, an attacker focus is seen as useful, addressing questions about what data attackers would be most interested in and what seems most valuable to them. Three participants also talk about levels of insecurity around emerging risks, e.g. an operational risk manager: "while we often encounter the same risks, the landscape is changing, with new risks emerging and risks we have never seen — leading to an uncomfortable position". At the same time, they advocate a proactive attitude to threats and risk, e.g. a threat intelligence manager stating that "as with all the models in the world, if you are not ready for something new, they are not helpful" or an operational risk manager demanding more decisive dealings with threats ('terminate' or 'transfer' risk instead of 'treat'[55]). Lastly and not directly related to an attacker focus, knowing the organisation and its systems including third party integration is seen as crucial — in the context of modelling, the requirement of "being specific" to the organisation is noted.

8.1.6 Perceived limitations to an attacker focus in practice

Several limitations to using attacker-centric approaches are stated in the interviews. As already indicated, participants see a limit to the amount of attacker information that companies like banks can source, and subsequently what threat intelligence insights they can obtain. As an example, dark web access is cited in the interview with the threat intelligence manager, which may have certain prerequisites, for example language skills (e.g. Russian) or specific capabilities to pass tests to gain entry to groups and appear as a criminal peer on these networks. Here, it is remarked that such specific intelligence could be provided by third-parties specialised in darknet intelligence who will have an active human actor presence in such networks. Secondly, a security executive sees a considerate downside to attacker representations in potentially reflecting personal bias brought forward by security professionals potentially, their experience and knowledge by overly focusing on one or certain attacker types ('pigeonholing') — this issue of potential bias is also supported by a senior manager in fraud strategy. And while one participant questions how much information around attackers from central intelligence teams is really trickling down into risk assessments, two participants describe an opposite effect, with tools often producing too much data to support analysis of aspects related to individual attackers; in "you can only do so much with limited resources" or "sea of transactions" (both from operational risk managers). This is also directly related to by a fraud executive sharing his frustration regarding a lack of industry-wide sharing of certain threat intelligence data, using the example of fraudulently used IPs or devices. Lastly, a

[55]This would relate to the '4Ts' approach of risk management, with ISO 27001 suggesting four ways to respond to risks: 'terminate' the risk by eliminating it entirely, 'treat' the risk by applying security controls, 'transfer' the risk to a third party, or 'tolerate' the risk [389].

threat intelligence manager reflects critically on what influences the uptake of attacker-centric approaches (mentioning visualisation tools to walk through attacks as an example), listing cost, shareability and comparability (an advantage inherent to common threat databases), real value and feasibility of practical implementation (cost/time/skills) as decisive factors for organisations when considering the adoption of such methods.

8.2 Researcher reflection on practitioner interviews

This section provides a brief reflection by the researcher on the completed interview process. In summary, 12 interviews with managerial level participants were completed successfully, with data collected from all interviews, and subsequently checked over and signed off by all participants for further analysis and usage. No technical problems were encountered, although several interviews had to be rescheduled at short notice due to diary changes on the participants' side. All participants were satisfied with the interview process and agreed to have their statements used (with small amendments in three cases) within the analysis for this thesis or other related publications.

This success was certainly helped by the researcher accommodating the interviewees (members of a 'corporate elite' as defined in Section 3.5.4) as much as possible (e.g. arranging times and meeting rooms in advance, working with personal assistants where applicable, not recording interviews where this was not wanted or sending polite reminders where further information was needed). Additionally, the actual interviews were kept to the minimum contact points, providing clear information beforehand including how many potential follow-ups were required — this was appreciated by most participants who generally have a busy and not very flexible schedule. To gain as much information as possible in these limited interview sessions, the researcher would aim to adopt and display an 'active listening' style, giving the participants as much time as possible to share their thoughts. The adopted feedback loop and member checking technique (refer to p.90), where the data collected was shared back with the participants for their feedback, proved crucial to ensure participants were entirely confident about their statements being accurate and used according to the ethical approval guidelines (refer to Section 3.5.4 and Appendix E), but also to collect additional data (for example where participants remembered further details or wanted to change specific sentences) and maintain a positive relationship with the participants. The second round of interviews (consisting of eight conversations to extend the original four) also helped to further establish patterns in the data, with participants confirming and corroborating aspects of attacker focus in each other's work, indicating an emerging level of theoretical saturation.

Finally, there was certainly a learning curve for the researcher: while the highest level of flexibility to accommodate the participants and their ideas had to be ensured a mostly free-flowing conversation, staying on topic without introducing limiting or leading questions (e.g. around the future of attacker-centric security) were paramount. This adopted conversation style meant that participants shared their thoughts not only on attackers, but security, risk or fraud topics within the digital banking domain — where useful and of interest, these are included in the last section, while the discussion in the next section aims to focus on attacker-centric aspects where possible.

8.3 Discussion and recommendations

8.3.1 Bringing together theory and practice

The following section attempts a comparative note considering both the insights from the literature review of attacker-centric approaches as provided in Section 2.1 and the results from the practitioner interviews as documented in the last section. And there seems to be a pronounced divergence in results: while the reviewed literature is largely focussed on modelling techniques and methodologies, the practical view is primarily concerned with the subject of the attacker itself. While the underlying research methods and questions will differ significantly between the interviews conducted and the reviewed research projects in Section 2.1, focus and terminology used also seem to vary in literature and practice. Lastly, a difference in mindset, and potentially a subconscious bias towards the expected outcomes, between academic researchers and practitioners can also be assumed: researchers will look to identify and synthesise patterns, while practitioners are trying to obtain usable and applicable insights. Looking at differences and similarities between theory and practice, this section then comments on the current status of the research area, segments out types of attacker-centric approaches and lists their benefits before concluding with a note on limitations and future potential.

Referring back to the literature review in Section 2.1, the current level of research activity around attacker-centric security approaches can be described as moderate, with only limited amounts of research studies directly focusing on this topic specifically in the literature reviewed. From the interviews with financial services practitioners a similar picture can be observed: while attackers certainly play a role in their security thinking, very few structured attacker-centric methodologies are mentioned. And while academic research addressing attacker categorisations as introduced in Chapter 6 can also be included in this research area, practical implementations or case studies of such categorisations actively in use in organisations seems sparse in the interview sample. In contrast, attacker personas as introduced in Chapter 7 of this thesis were mentioned in both literature and by several practitioners (see note in Section 8.1.3).

Furthermore, while threat modelling as a methodology seems readily understood and informally employed by many of the practitioners interviewed, no significant level of formalisation of such approaches is evident — this is in strong contrast to the literature reviewed, where research output would often be linked to frameworks or models (Section 2.1). Conversely, authors of the reviewed literature seem to have accepted the concept of an attacker focus or attacker-centric security approaches without much questioning, while practitioners seem to be actively debating the role of attackers in their thinking.

With both literature as presented in Section 2.1 and the practitioner interviews in Section 8.1 yielding interesting results in regard to attacker-centric approaches, the next paragraph categorises and summarises the types of attacker-centric approaches and thinking encountered across these two samples. To help structure the collected data and observed information on attacker-centric approaches in security from both literature and interviews with practitioners, the following four tentative categories and labels can be devised. It should be noted that the

boundaries between these groups are most likely to be fluid, due to the large variation in the level of attacker focus found in the samples.

Subconscious or hidden attacker thinking — firstly, attacker focus may simply take place in the context of existing approaches, for example in practical threat intelligence, but also have an influence on well-known threat modelling techniques (e.g. STRIDE). While attackers do not explicitly form part of such approaches, they are likely to be part of the model the 'modeller' has on their mind — this can potentially be described as 'subconscious or hidden attacker thinking'.

Abstract attacker thinking — another variant of thinking about attackers can be viewed as 'abstract attacker thinking' — this is predominantly found in literature examples, where relatively abstract attacker representations (without described characteristics and behaviours) are used, for example attack trees, misuse cases or attack patterns.

Integrated attacker thinking — approaches with a stricter attacker focus and integrating more detailed attacker representations can be identified in the sample — such 'integrated attacker thinking' can for example be found in uses of the cyber kill chain methodology (both in literature [99][390] and in the conversations; also refer to p.28), where attacker behaviours across the seven stages of the kill chain are evaluated. Other approaches with a strong element of attacker thinking, although not necessarily focussed on details or related real-world data, include customised threat scenarios (as discussed in the practitioner interviews), detailed attacker categorisations or threat libraries (in the literature review, e.g. [71][74][85]).

Dedicated or advanced attacker thinking — lastly, there are the truly, 'dedicated or advanced attacker thinking' approaches like attacker personas (in the literature review, e.g. [7][44][45] and mentioned by interview participants); also discussed at length in Chapter 7) as well as models and simulations based on existing groups and past incidents (as discussed in the interviews).

Building on the types of attacker-centric approaches described in the last paragraph, what is their purpose and benefits as described in literature or perceived by practitioners in the field? To summarise the stated benefits from both literature and practitioners accounts, the following five themes can be identified.

Knowing your enemy (and their business) — at the most basic level, attacker-centric thinking and related research methods can be seen to aid the understanding of attackers or to "provide general insight into the attacker's mind" [74]. In the interviews with practitioners, this was extended to not only gain an understanding of the attackers as individuals or groups, but their entire ecosystem and criminal business model. This ability to further comprehend cyber operations through focusing on actors involved was highlighted by all practitioners, but not mentioned explicitly in the literature sample.

Supporting a strategic view to security — another aspect predominantly mentioned by the practitioners is the strategic view on threats and security. In practice, attacker information including group structure, capabilities and preferred attack vectors (even if past incidents and involved actors are used only as examples) is seen as helpful for a proac-

tive look into future potential threats to a system. This is in line with Shostack ([6] p.40; also [65]) viewing an attacker-centric approach as unsuitable for threat modelling purposes at a granular system level (refer also to Section 2.2). It may therefore be the case that attacker-centric approaches are of value for supporting higher-level security strategy, but do not provide the necessary structure to support the modelling around the question of 'what could go wrong?' with a system — methods like STRIDE or threat lists (e.g. CAPEC[56]) may be better suited [392].

Creating reusable attacker reference frameworks — in close relation to the last point, several literature items class the creation of generic, reusable attacker reference libraries as useful for security practice [74][85]. This view is supported by a statement from a senior threat intelligence manager in the sample — examples of attacker groups, also based on existing groups and known incidents, are deemed useful for modelling and reference purpose. Practitioners also describe the value of working together across the organisation and also industry-wide, requiring shareable, data-based insights relating to attackers and their activities such as e.g. attack path maps.

Identifying and modelling threats (alongside other approaches) — in the most direct sense, attacker-centric approaches may help to identify potential threats, for example through social media monitoring where explicit or vague threats against the organisation by potential attackers get picked up and can be assessed. Attacker-centric thinking is seen to support the prioritisation of threats [44], testing of new countermeasures [74] through threat scenarios (in interviews) or the evaluation of security decisions [45][66]. A statement from one of the interview participants (security executive) seems insightful in this context: the level of determination to succeed displayed by attackers behind an attack may strongly define the strategic defence response.

Enabling stakeholder communications — attacker-centric approaches may also help communication with stakeholders, which is mentioned in both literature and conversations with practitioners. Reassurance of stakeholders is mentioned as a key element in threat intelligence — this is likely to include an element of attacker information. Attacker information is also seen as a confidence building element for stakeholders in the literature [73] — this is certainly an interesting human and organisational element in relation to attacker-centric approaches. Additionally, talking about attackers and working with attacker-based models is viewed as useful for daily communication and collaboration of security efforts across multidisciplinary teams [45][66][70], but also for security-related training and awareness campaigns (as mentioned by a threat intelligence manager).

Sections 2.1, 2.2 and 8.1.6 have discussed several limitations to attacker-centric approaches as observed in the reviewed literature or shared by practitioners, and some points can be highlighted when comparing these perspectives. While attacker-centric approaches seem to be of limited use for highly structured and efficient threat modelling frameworks, this drawback

[56]The Common Attack Pattern Enumeration and Classification (CAPEC) list, trademarked by the MITRE corporation, provides "a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities" to be "used by analysts, developers, testers, and educators to advance community understanding and enhance defenses" [391].

seems to have been overcome by security practitioners using them for a different purpose in their organisations: to implement and use this information in their efforts to create a more strategic view on current and future threats. Another interesting point is the practical challenges of sourcing information and intelligence from darknet sources — such restrictions (or others such as cost, scalability or internal skillset) are issues not considered in the theoretical works reviewed, but seem very relevant in practice. Lastly, the potential problem of bias in security professionals when thinking about certain attacker types raised in the practitioner conversations is actually directly addressed by the reviewed literature items involving attacker personas [7][44][45]. In particular, Atzeni et al. [7] consider attacker personas as a way of mitigating individual bias, basing this assessment on similar insights in user-centred design (where conventional personas originate from).

A number of proposals for future research in this area have been made in Sections 2.1 and 8.1.5 and are also integrated in the recommendations and guidance for using attacker-centric approaches in the next section. To highlight a few central points, integration of attacker-centric methods and techniques into daily development practices (including agile ways of working) in organisations seems crucial to offer real future value to practitioners — tools or reusable attack pattern libraries and attacker type representations may also be of interest in this context (as mentioned in [9][62][79][97], but also indicated in interviews). There may however also be a convergence of both theoretical and practical perspectives in future, with practitioners seeing a further move towards data-driven attacker modelling efforts and emerging technologies on the rise — here, one interviewee remarked on academic efforts 'already discussing these attacks in theory'. The potential for using attacker-centric approaches for collaboration, training and communication purposes also requires further investigation (in [45][66][70][77][99] and also mentioned by participants): here, Chapters 6 and 7 of this thesis have provided an example of such approaches with a practical, sector-specific focus in preparation for further evaluation. In direct relation, the understanding and integration of the element of 'attacker determination' in existing attacker categorisations (e.g. in Hald & Pedersen [24], Seebruck [25] or our typology in Chapter 6) may prove to be an interesting point for future research.

8.3.2 Guidance on effective usage of attacker-centric approaches

Based on the learning and discussion points raised in this chapter so far, a list of recommendations and guidance points on the usage of attacker-centric approaches in security is offered in this section. The intention for this is twofold: firstly, this is seen to support ways of using such approaches effectively in security practice. Secondly, this list is seen to help set future research directions and suggest new practical ways of incorporating attacker thinking in theory and practice. While these suggestions are at an early stage, it is nevertheless hoped that this list is considered of value as a discussion basis for practitioners and researchers alike, e.g. when initially considering attacker-centric approaches in their organisation or research, to help compare their experiences and findings and to ultimately challenge this list.

Based on the presented results and stated discussion points, the following 12 points should be taken into account when working with (or planning to work with) attacker-centric approaches:

1. *Consider attacker-centric approaches to develop a strategic view on threats and security.* A key insight gained from the analysis in this chapter is the usage of attacker-centric approaches in a strategic sense. Using models of attackers or attacker groups (even informal ones) and related threat scenarios may potentially help to develop a strategic view on current and future threats. While the actual implementation for such an approach is likely to vary across organisations and further research would be beneficial, this insight seems to be of significant practical value. It also aligns with the understanding that attacker-centric threat modelling is often ineffective: it may ultimately be better suited for another purpose like supporting a strategic view on security.

2. *Recognise and accept limitations for attacker-centric approaches.* While this thesis has spent significant effort discussing attackers and attacker-centric approaches, the limitations of such approaches need to be understood if they are to be used effectively. Although these limitations may differ for the context of application, one of the most important realisations is certainly the perceived ineffectiveness of attacker-centric approaches for structured threat modelling — here, approaches deconstructing the system and data flows (e.g. STRIDE or PASTA threat modelling, discussed in Section 2.2) may provide better guidance to most modellers.

3. *As an academic, learn from security practitioners (and vice versa).* The analysis in this chapter shows a discrepancy between academic research themes and topics that matter most in daily practice: while formalisations and frameworks dominate the academic space, daily security practice includes threat intelligence approaches and far more informal modelling efforts. It is felt that both sides would benefit from bridging this disparity, with an interest in academic research also indicated in the practitioner interviews. While academics should be looking at some of the points raised by practitioners in this analysis (e.g. work routines, their thinking about attackers and informal modelling of attacker groups), they would in turn potentially benefit from further formalising their approaches, e.g. for reusability or shareability across the industry.

4. *Benefit from attacker-centric approaches to understand attacker ecosystem and criminal business models.* While this point was highlighted by practitioners, it was not evaluated in much detail in reviewed academic materials — this seems like a missed chance and further research in this area would be of value, for example to assess the exact benefit provided by such approaches, but also potential methods and procedures that can be used in this context.

5. *Choose from a range of attacker-centric approaches with varying levels of formality and required effort.* To integrate attackers into daily security practice or academic research, there are a variety of methods and techniques to choose from, for example abstract attacker models, attack path maps, attack trees, misuse cases and threat scenarios, but also attacker personas or typologies. It is also crucial to realise that attacker-centric approaches can be implemented to varying degrees — they may supplement existing methods or form a fundamental part of a security programme.

6. *Use attacker-centric approaches as a communication or training tool.* The often visual nature of attacker-centric approaches like attacker personas, typologies or digital

journey maps may help to explain current security trends to senior stakeholders, e.g. provide assurance around media reports or to make a case for security spending. These attacker-centric tools may also play a role in training exercises with security and non-security teams, e.g. to raise security awareness or evaluate current work practices.

7. *Actively look for and address potential biases present in security teams.* Personal bias may be present in security teams when thinking about attackers — individuals may for example over- or underestimate the threat originating from certain attackers or attacker groups (based on experience or knowledge). This potential presence should first be acknowledged and secondly countered if possible — personas are seen as a method to address such biases in user-centred design and hence may also be of benefit in an information security context.

8. *Consider attacker entry points in the (online and offline) digital customer journey.* Practitioners working in the area of digital banking in our interviews place great emphasis on the model and visualisation of the digital customer journey as a series of steps customers will move through when completing a bank service or sales processes. Mapping attackers, their activities and resources (for example in the form of attacker typology types, personas or path maps) against this sequence may help to identify potential vulnerabilities and attack entry points when assessing existing journeys, but also changes to be made or entirely new innovations. This highly customised and accessible approach may help to connect digital professionals such as designers and product managers as well as security experts to help better balance business, customer and security needs. As formalised approaches and reflective case studies discussing such approaches are limited at this point in time, with academic literature not considering the commercial concept of customer journeys adequately, further research in this area should be considered, ideally in collaboration with business practitioners.

9. *Integrate attacker-centric thinking into the assessment of emerging technologies.* As ML and AI have moved from theoretical concepts into practice used by banks, attacker-centric thinking may also help when identifying and assessing threats, risks and the related need for new security controls. In a business context, digital journey mapping as mentioned above incorporating these new aspects (e.g. chat bots as already commonly used across the UK banking industry, e.g. [393]) may also support such efforts.

10. *Start thinking about how attackers and threat modelling can be built into agile ways of working.* As agile ways of working with multidisciplinary teams become more widespread across organisations around the world, ways of integrating threat modelling into these processes need to be identified. Davoust in [394] has suggested for teams in organisations to be trained to use agile and continuous threat modelling and uses an attacker profiling exercise to support this. Collaboration within and between teams throughout the development process seems crucial in this context, recognising that everyone is responsible for security and it needs 'to be built in' rather than 'bolted on'. While no comprehensive frameworks around this have been found here, concepts such as evil user stories ("As a hacker, I can send bad data in HTTP headers, so I can access data and functions for which I'm not authorised", in OWASP [395]) seem like an interesting starting point to combine attacker-centric and agile approaches to security.

11. *Collaborate around attacker-centric thinking and share attacker-related information.* Threat intelligence and the sharing of attacker information should underlie the concept of attacker focus in practice across the organisation, and beyond where possible. This should be extended into collaboration efforts around attacker focus, both within organisations (e.g. through agile working sessions examining digital journey maps and attacker entry points) or in the form of industry-wide initiatives and working groups. Effective tools and techniques enabling such sharing and collaboration efforts have also been discussed widely in literature, e.g. attacker typologies or personas as also discussed in this thesis, but also threat and attack pattern libraries (e.g. Intel Threat Agent Library [22] or CAPEC [391]; also in Section 2.2) — re-using such existing frameworks can also enable scalability, comparability and reduce duplication of efforts.

12. *Publicise insights and learnings in this area to support others.* Given the limited amount of research currently presented, further practical and academic efforts seem required to advance this field of research. Considering the amount of valuable statements from only a small number of initial interviews, there seems to be significant potential for further insight to be gained. It is therefore crucial that practitioners consider making some of their learning and experiences public, for example through presentations at industry-specific or academic conferences.

8.4 Conclusion and reflection

This chapter has looked at the current status of attacker-centric approaches in security in both theory and practice. From the analysis results, reflection, discussion and guidance notes provided so far in this chapter, the following points can be highlighted in summary of this research on attacker-centric security, also referring back to previous chapters of this thesis.

Further definition of expected benefits required — exact benefits and outcomes associated with the usage of attacker-centric approaches often remain unclear, as indicated by the reviewed literature items in this research (Section 2.1, 2.2.3 and 2.3). There seems to be an underlying assumption that knowing more about attackers is helpful in the context of modelling threats and supporting security practice in general, although the exact motivation and the 'why?' behind using attacker-centric approaches are often relatively vague.

Many different methods currently in existence — current approaches which use attacker information or employ an attacker focus vary significantly in terms of effort required as well as rigour and detail involved. Hence, there seems to be a significant potential for unification and formalisation of tools and techniques, with the aim of establishing options for reusability, comparability and shareability.

Changing perspectives to a more strategic outlook — the proposition of using attacker-centric approaches to support a macro-level strategic view of practitioners is certainly worth considering. It is in contrast to the principle of using attacker information for threat modelling at a granular level — an approach which has been criticised over recent years as ineffective in comparison to system- or security-focussed efforts. Assigning a

specific purpose to attacker-centric approaches could also help to solve the first two issues mentioned here, potentially supporting consolidation and further concentration of existing methods. Beyond this research, there are certainly signs that this could be the future direction for attacker-centric approaches: e.g. in Krebs [396], who sees actor attribution as a key intelligence aspect as malware evolves.

Attacker categorisations and types mentioned throughout theory and practice — descriptions of various attacker groups, categories and types are mentioned in both the literature review in Section 2.1 as well as the interviews (although specific usage typologies are not mentioned in this context). Additionally, the practitioner interviews also introduced a new potential descriptor for attackers: the level of determination, describing how far attackers are prepared to go and whether mitigations will deter them. This element could easily be added to describe and classify attackers in future attacker typologies, potentially also in a new iteration of our typology as introduced in Chapter 6.

Cautious, but positive outlook on attacker personas in theory and practice — further to the practitioner perspective on attacker personas collected via a larger-scale survey amongst financial services professionals in Chapter 7, this chapter has also seen practitioners in the in-depth interviews mention this vehicle for attacker modelling. While the work presented in Chapter 7 has highlighted the ability of attacker personas to 'bring attackers to life' and make them more accessible, tangible and realistic to a wide range of security stakeholders, the literature review also sees them as a support tool for communication and collaboration (in Tariq et al. [45]) or to help mitigate potential bias (in Atzeni et al. [7]) in organisations. While practitioners in this chapter show interest in using attacker personas, experiences of working with them seem limited — here, aligning them to representations already used by a variety of teams across the agile organisation like digital journey maps may provide an entry point for future research.

Attackers play a (limited) role in daily work routines — summarising on this chapter and based on the limited sample of interviewed practitioners (this aspect is not addressed in detail in the reviewed literature), thinking about attackers plays some role in the daily work routines for financial services practitioners. This may take a number of forms, e.g. through threat intelligence reports distributed across the organisation, usage of threat scenarios or examples of attacker groups, also depending on the individual role of the practitioner. It is important to understand that this role is limited — reasons mentioned are e.g. time constraints and different focus in their overall job role, but also a lack of perceived practical value or related tools available to them.

Integrating security into digital experience management — practitioners in our interviews placed high importance on business requirements, but also user needs, related to the digital journey and experience of (potential) customers to the bank. In this context, visualisation and mapping techniques such as customer journey maps, attack path maps and attacker personas are mentioned to support the alignment of business, user and security needs, also fitting into the academic research areas of usable security or human-computer interaction for security.

Part IV

Conclusion

9

Future Work

This brief chapter proposes ideas and directions for potential future work which have arisen during the research process undertaken in this thesis.

The future work identified for this thesis can be seen to broadly fall into the following five areas, which are briefly outlined in turn in this chapter:

- the addition of new and updated data sources to the original dataset;
- a methodological extension of the methods used in this thesis;
- further stakeholder collaboration, validation and dissemination;
- further investigation into the potential of attacker-centric approaches in a strategic context; and lastly
- research on ways to make attacker-centric approaches useful and effective for (financial services) practitioners.

Firstly, further data sources (e.g. primary data through interviews with cybercriminals or data made available directly by financial institutions) could be added to the dataset used in Chapters 4 and 5 (and as a basis for subsequent chapters) to help substantiate the results achieved from the publicly available data. Reviewing and updating the current dataset on an ongoing basis may also help introduce and reflect new trends and developments (e.g. in the area of fintech innovations, blockchain applications or cryptocurrencies). Adding this new data may especially help to corroborate aspects of attacker characteristics and behaviours marked as tentative due to limited evidence in the data (as raised in Sections 4.4 and 5.4), e.g.

psychological traits or self-perception of attackers, elaboration on cybercrime business models or decision-making for selection of targets and general victimology. Lastly, adding further interviews with practitioners from financial services institutions beyond the case company used in Chapter 8 could help strengthen the methodological grounding of this study — this focus on only one institution has also been a point of criticism in the reviewer comments for the publication of results for Chapter 8 in [397] and should therefore be addressed when building on and developing this study further.

There are further opportunities for methodological improvement and extension of the methods used in this thesis. Also in relation to the last point, replication efforts using the methods suggested in this thesis (or adapted variants) using new data or alternative settings may offer interesting starting points for future research. Attacker typologies could be extended to other industries, while specific attacker groups or other subcategories could be refined further — experiments around new visualisation options may also show potential in this area. As indicated in Chapter 7, the attacker persona set should be progressed through further iterations cycles, with the aim of moving from generic profiles to more specific attacker representations and situations, also addressing potential stereotypes where possible. Several new aspects brought forward by practitioners in Chapter 8 also show potential for future examination, e.g. the end-to-end modelling of the digital journey to visually map and conceptually align business, user and security requirements, where attacker personas may find entry alongside their traditional user persona counterparts.

It is also expected that the research conducted in this thesis would substantially benefit from further stakeholder collaboration, validation and dissemination. Extending on the review and feedback received for the attacker personas through a survey study, further validation from a selection of subject matter experts (for example financial services security personnel, law enforcement professionals or other practitioners as well as academics in the field) may help to further validate and potentially improve these attacker representations in the future. Such collaborative exercises could also demonstrate the practical value of attacker-centric approaches for training and communication in the context of security awareness — this topic may also serve as a starting point for further academic research.

The potential benefit of such collaborative research approaches is already subtly implied in the conversations with practitioners: ‘attacker determination’ is deemed as a crucial element to assess and model attacker groups by the interviewed financial services senior managers, although this criterion is not adequately reflected in current academic attacker typologies. While such statements naturally require further careful investigation, these examples illustrate how input from practitioners may challenge and disrupt accepted methodologies — ultimately leading to positive change and progress in this area and bringing academia and industry closer together.

Another central point of this thesis has been the realisation that, while they may not be suited for granular, low-level threat modelling processes, attacker-centric approaches such as attacker typologies or personas can support a more strategic, high-level perspective on the security of a given system. This insight offers a logical explanation regarding the effective positioning of attacker thinking in security and aligns with the assumptions commonly made in threat modelling literature — system-centred approaches are generally preferred over attacker or

asset focussed threat modelling (as laid out in Section 2.2). However, while this understanding is intriguing and offers interesting potential for future research and practice in the area of threat intelligence and modelling, the available evidence is currently limited — also in this thesis. Further research with the aim of grounding this output in data (e.g. with further primary research through interviews) is therefore strongly advised.

Lastly, if practitioners are to benefit from this strategic perspective on current and future threats, attacker-centric approaches need to work for them in their daily practice. Future research efforts may consider the integration of such methods into current project management methods including agile ways of working, but also the creation of tools and reusable patterns that make the adoption of such approaches easier for practitioners working in the field (e.g. accessible adaptations of attacker persona methods). To avoid attacker categorisations such as typologies and personas turning into 'stand-alone' methods disconnected from everyday practices around security and risk assessments, their practical value and fit for organisations needs to be examined and considered in further detail. As interviewees in Chapter 8 mention themes such as increasingly complex and interconnected systems, data-driven attacker modelling and emerging technologies as future risks and opportunities, research at this intersection of academia and industry can be expected to strongly support practitioners, with both theoretical and practical perspectives potentially converging further in future.

10

Conclusion

This chapter forms the conclusion of the thesis, synthesising the key research findings and contributions from this work. Furthermore, it relates the obtained results back to the initial research aims, objectives, questions and expected contributions as set out in the introduction chapter, also reflecting on the research process from the researcher's perspective.

The main purpose of this thesis has been to conduct a detailed investigation into attacker-centric approaches in security as well as the exact nature of digital banking attackers. Here, prior research and practitioners' views have also been considered to evaluate the usefulness of attacker-centric approaches and to provide recommendations for their optimal usage as well as potential future research options in the area. Concluding this thesis, this chapter summarises and reflects on the findings and contributions made in this work, also comparing them to the initially set out research objectives and questions as well as expected contributions (in Chapter 1). To achieve this, the key research findings, outcomes and contributions identified for this thesis are stated and compared to the expectations stated in Section 1.5. Following this, the research questions and questions from Chapter 1 are briefly re-introduced (in Table 10.1) and examined against the outcomes ultimately presented in this thesis. As part of this assessment, a brief reflection by the researcher as to what extent the research questions and objectives have been met is also provided.

The following key research findings, outcomes and contributions can be identified:

Definition and re-positioning of attacker-centric approaches as a strategic viewpoint —
Under consideration of prior research and with input from a senior group of financial services practitioners, Chapter 8 has been dedicated to an evaluation of attacker-centric approaches as currently used in a security context, supported by a systematic review of related literature in the background section of this thesis. This grounding has helped to highlight differences in thinking about attackers employed by academic researchers and practitioners: an increase in collaboration and research with a practical motivation is seen as beneficial here. As a tangible outcome, guidance points on the effective usage of attacker-centric approaches have been provided in this chapter. One of the key insights in this chapter, albeit tentative at this point in time pending further research, has also been the realisation that attacker-centric approaches and thinking might be most suited to support strategic perspectives. This is in contrast to system-centric threat modelling approaches looking to decompose the system's architecture to identify threats. This could be an impactful finding: if this statement can be further corroborated and these new ways of using attacker-centric approaches can be formalised, this would potentially influence researchers in the area of threat modelling and their future work. These findings have been published by the researcher in [397], with methodological aspects also discussed in [282].

Definition of attacker groups (typology) relevant to digital banking —
Using the information on attackers from previous chapters, Chapter 6 has set out to categorise and group attackers together forming a typology in line with prior literature in this field. However, rather than purely adapting and extending existing methods and categories, the presented research has built an independent typology specific to digital banking. Additionally, validation efforts are suggested and completed within this work, providing a further iteration including initial amendments of the attacker typology. A further contribution has been made in the form of a dedicated excursus on circumplex models, critically assessing this visualisation employed in previous literature. These results have been published as [275] and [276].

Presentation of attacker personas specific to digital banking —
Chapter 7 has integrated the proposed attacker typology for digital banking from Chapter 6 into a process model borrowed from user-centred design for building attacker personas. However, the focus of this research has been on the output and the presentation of comprehensive and convincing attacker persona representations for an applied business case, aiming to raise the level of quality and detail of attacker personas in a security context closer to the level applied to user personas. To evaluate the perception of the proposed attacker persona set amongst financial services practitioners and understand the overall acceptance of the general method in this group, a survey study has been carried out, showing interesting potential for communication and training purposes, but also methodological challenges. Beyond this thesis, further in-depth evaluation and collaborative persona building exercises will be of benefit in the future, also starting the next iteration cycle of this attacker persona set. The initial iteration of this attacker persona set has been published as [280] and [281].

Research objective	Research question	Ch.
(1) Provide a detailed, but focussed enquiry into research surrounding attacker-centric security approaches.	**(1)** What role does attacker focus and usage of attacker information play in security literature?	2
(2) Define a set of methods to serve as a comprehensive research design framework for this research project.		3
(3) Establish a comprehensive picture of attackers targeting digital banking services, their characteristics and behaviours.	**(2)** Which common characteristics and behaviours can be identified for attackers targeting digital banking systems through data analysis?	4, 5
(4) Construct a digital banking specific attacker categorisation, extending the analysis of real-world digital banking attackers.	**(3)** In line with previous research in the area of attacker categorisations, how could a set of attacker types look?	6
(5) Develop a set of attacker personas specific to digital banking building on the insights previously gathered.	**(4)** Building directly on the results from data analysis, how would a complete and detailed set of attacker personas be defined and visualised?	7
(6) Further explore the state of attacker-centric security, methods and tools in practice and synthesise these insights into suggestions for guidance.	**(5)** How are attacker-centric security approaches used in practice and what value do they provide to security practitioners in financial services?	8

Table 10.1: ***Summary of research objectives and questions with thesis chapters***

Provision of a grounded understanding of digital banking attackers —

A key contribution and starting point for subsequent chapters in this thesis is the detailed analysis of characteristics and behaviours of digital banking attackers in Part II, based on a grounded theory method analysing over 300 publicly sourced materials from a dataset consisting of four different publicly available data sources. These results have directly supported later studies in Part III of this thesis, but also provide an independent, tangible research outcome, which may be of interest to other researchers. Potential secondary contributions have been a demonstration of the value of publicly available data as well as the provision of a case study for grounded theory usage in a security context, which peers may be able to reference and build on in the future.

Given this list of findings and contributions, how do these then help to answer the research questions and meet the objectives set for this research in Chapter 1? This section restates a shortened version of the research objectives and questions in summary (in Table 10.1; from Chapter 1) and explains how and to what extent it is felt these have been addressed within this thesis.

Research Objectives 1 and 2 as well as Research Question 1 have been answered directly by the provision of an initial literature review in Chapter 2 and Chapter 3, summarising the methodology and research design underlying the entire research project.

For Research Objective 3 and Question 2, Chapters 4 and 5 have provided a structured approach and detailed account of characteristics and behaviours of digital banking attackers grounded in data. It is felt that the research questions and objectives stated have been answered in principle, providing several contributions as stated above: a data-driven and detailed overview of attackers specific to the case of digital banking and furthermore, a demonstration of the value of publicly available data and also grounded theory as an analysis strategy for this type of research. At the same time, it is felt that these data sources limited this research in some instances: for example, due to the relative age of some of the sources, very recent threats, attacks or threat actors applicable to digital banking may not have been sufficiently considered. Furthermore, while the grounded theory methods used in this context have brought forward some interesting aspects that would warrant further enquiry (e.g. victimology specific digital banking fraud), many of these issues have lacked the depth of references to form a comprehensive picture (e.g. certain legal aspects and fraud liability) and would benefit from further research outside of this thesis (potentially with a different source dataset).

Research Objective 4 and Question 3 have been addressed in Chapters 6 and are considered as being met by the proposal of the attacker typology in Chapter 6. It is felt that the results provided and published as [275] and [276] fit closely into the related area of research (attacker categorisations) and will be of interest to others interested in this field — here, the excursus on circumplex models may also help others considering work in this area potentially using this type of visualisation. While an initial level of evaluation through peer review and heuristic assessment have been completed, further validation efforts, also leading to further updates and iterations of the typology may be useful. Additionally, the overall reasoning behind building and using attacker categorisation could benefit from further investigation and clarification — the presented typology is not exempt from this limitation (although Chapter 8 has addressed this issue partially). Lastly, Chapter 8 has also provided an interesting insight relevant to attacker categorisations: attacker determination has been mentioned as a factor to describe and model potential attackers on. Current categorisations including typologies like ours only accommodate this aspect to a certain degree and further examination into the potential of this aspect could prove interesting in the future.

In answer to Research Objective 5 and Question 4, Chapter 7 has presented a set of attacker personas specific to digital banking, elevating the relatively abstract attacker representations of the typology to more detailed, human presentations of potential attackers to a system (digital banking in the case of this thesis). This attacker persona set has received overall positive feedback at academic conferences [280][281] and from practitioners directly (also in Section 7.3). While a first iteration cycle has been completed and several resulting amendments have already been included in this thesis, further iterations to develop, further specify and improve these personas are envisioned. Ideally, a future industry collaboration could see these attacker personas placed in real-world organisation, with multidisciplinary, agile teams making use of this tool — here, the integration of attacker personas into common UX practices used in digital organisations such as journey or service maps could also offer interesting starting points for future academic research.

Research Objective 6 and Research Question 5 have been addressed in Chapter 8 and it is felt that a tangible outcome has been achieved and published in the form of guidance around attacker-centric approaches, based on conversations with an interesting panel of senior practitioners in financial services [397]. Several findings in this chapter have certainly been thought-provoking and can be considered as excellent starting points for future research in an area with limited previous research. For this thesis, it is also felt that there is a certain level of disparity and lack of integration with earlier chapters in Part II, with not many of the insights from Chapters 4 and 5 being capitalised on in this chapter (although earlier materials are referred to in the discussion in Section 8.3). Also focussing on the positive insights and ideas from this chapter, further substantiation of this topic is seen as useful (as outlined in Chapter 9). This could for example include further dedicated research regarding attacker-centric approaches and their strategic role in security thinking in the future.

Overall, this thesis has drawn attention to the topic of attacker-centric thinking in security, which had not received much dedicated treatment previously, leaving the area between the two extremes of the common paradigm of 'thinking like an attacker' and strong opinions against attacker-centric threat modelling. This work has aimed to describe and define this situation, including tools used in an attacker-centric context such as attacker categorisations and personas, all grounded in data from a real-world sample in the area of digital banking. Working with financial services practitioners, opportunities, benefits, limitations and boundaries of attacker-centric approaches and thinking have been assessed, also synthesising these findings into a list of suggestions on how to implement and benefit from such a focus in everyday work practices. At a theoretic level, this work has crossed over into the area of HCI research, also indicating the potential of integrating such approaches in organisational practices, including contemporary agile working processes — at the same time, this work has also been placed in the context of existing bodies of research in the areas of threat modelling, attacker categorisations and personas where possible. With this in mind, abstracting and modelling attackers as an inherent part of every attack and security problem will always pose a challenge to practitioners and researchers: ultimately, human threat actors may behave in their own, often unpredictable ways, while the human users of systems that we are trying to protect and secure do not always adhere to rules, convictions and expectations we may have.

Bibliography

Bibliography

[1] B. Christianson, J. Malcolm, V. Matyas, and M. Roe, eds., *Security Protocols XVI: 16th International Workshop, Cambridge, UK, April 16-18, 2008. Revised Selected Papers*, vol. 6615 of *Security and Cryptology*. Springer, 2011.

[2] M. Howard and D. LeBlanc, *Writing Secure Code 2*. Microsoft Press, 2nd ed., 2003.

[3] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Uncover Security Design Flaws Using The STRIDE Approach." `https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach`, Nov. 2006. Last accessed 1st August 2020.

[4] N. Shevchenko, "Threat Modeling: 12 Available Methods." `https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html`, Dec. 2018. Last accessed 1st August 2020.

[5] A. Shostack, "Experiences threat modeling at Microsoft," *Modeling Security Workshop*, 2008.

[6] A. Shostack, *Threat Modeling: Designing for Security*. John Wiley & Sons, UK, 2014.

[7] A. Atzeni, C. Cameroni, S. Faily, J. Lyle, and I. Fléchais, "Here's Johnny: A methodology for developing attacker personas," in *Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security (ARES'11)*, (Vienna, Austria), pp. 722–727, ACM, Aug. 2011.

[8] G. Martins, S. Bhatia, X. Koutsoukos, K. Stouffer, C. Tang, and R. Candell, "Technical Report: Towards a Systematic Threat Modeling Approach for Cyber-physical Systems," in *Proceedings of the 2015 Resilience Week (RSW)*, 2015.

[9] P. Meland, E. Gjære, and S. Paul, "The Use And Usefulness of Threats in Goal-Oriented Modelling," *Proceedings of the 2013 Eighth International Conference on Availability, Reliability and Security (ARES'13)*, pp. 428–436, Sept. 2013.

[10] C. Moeckel and A. E. Abdallah, "Threat modeling approaches and tools for securing architectural designs of an e-banking application," in *Proceedings of the 2010 Sixth International Conference on Information Assurance and Security (IAS'10)*, (Atlanta, Georgia, USA), pp. 149–154, Aug. 2010.

[11] M. Palanivel and K. Selvadurai, "Risk-driven security testing using risk analysis with threat modeling approach," *SpringerPlus*, vol. 3, no. 1, p. 754, 2014.

[12] B. Potteiger, G. Martins, and X. Koutsoukos, "Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment," in *Proceedings of the 2016 Symposium and Bootcamp on the Science of Security (HotSos'16)*, (New York, NY, USA), pp. 99–108, ACM, 2016.

[13] M. Surridge, G. Correndo, K. Meacham, J. Papay, S. C. Phillips, S. Wiegand, and T. Wilkinson, "Trust Modelling in 5G Mobile Networks," in *Proceedings of the 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges (SecSoN'18)*, pp. 14–19, ACM, 2018.

[14] N. R. Mead, F. Shull, K. Vemuru, and O. Villadsen, "A Hybrid Threat Modeling Method," Tech. Rep. CMU/SEI-2018-TN-002, Carnegie Mellon University Software Engineering Institute, `https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617`, 2018. Last accessed 1st August 2020.

[15] A. Kayem, R. Ratshidaho, M. L. Maoyi, and S. Macanda, *Information Security in Diverse Computing Environments*, ch. Experiences with Threat Modeling on a Prototype Social Network, p. 19. IGI Global, 2014.

[16] N. Munaiah, A. Rahman, J. Pelletier, L. Williams, and A. Meneely, "Characterizing attacker behavior in a cybersecurity penetration testing competition," in *Proceedings of the 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM'19)*, pp. 1–6, 2019.

[17] P. Johnson, A. Vernotte, M. Ekstedt, and R. Lagerström, "pwnPr3d: An Attack-Graph-Driven Probabilistic Threat-Modeling Approach," in *Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES'16)*, pp. 278–283, ACM, 2016.

[18] C. Harber, "How to Think Like an Attacker." `https://www.bankinfosecurity.com/interviews/how-to-think-like-attacker-i-4492`, Oct. 2019. Last accessed 1st August 2020.

[19] E. Heymann, B. P. Miller, and L. Kohnfelder, "Introduction to Software Security — University of Wisconsin course materials." `https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/`, 2019. Last accessed 1st August 2020.

[20] O. Saydjari, "Security engineering course homepage — Johns Hopkins University." `https://apps.ep.jhu.edu/course-homepages/3667-695.614-security-engineering-saydjari`. Last accessed 1st August 2020.

[21] R. Hurlbut, "User-Story Driven Threat Modeling (presentation recording and notes)." `https://www.youtube.com/watch?v=oEfOKK895Q8` or `https://roberthurlbut.com/r/CM19USTM`, 2019. Last accessed 1st August 2020.

[22] Intel Corporation, "Threat Agent Library Helps Identify Information Security Risks." Available via: `https://www.researchgate.net/publication/324091298_Threat_Agent_Library_Helps_Identify_Information_Security_Risks`, Sept. 2007. Intel Information Technology White Paper. Last accessed 1st August 2020.

[23] M. K. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy," *Digital Investigation*, vol. 3, no. 2, pp. 97–102, 2006.

[24] S. L. N. Hald and J. M. Pedersen, "An Updated Taxonomy for Characterising Hackers According to their Threat Properties," in *Proceedings of the 14th International Conference on Advanced Communication Technology (ICACT'12)*, pp. 81–86, 2012.

[25] R. Seebruck, "A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model," *Digital Investigation*, no. 14, pp. 36–45, 2015.

[26] M. de Bruijne, M. van Eeten, C. H. Ganan, and W. Pieters, "Towards a new cyber threat actor typology — a hybrid method for the NCSC cyber security assessment." TU Delft, 2017.

[27] S. Faily and I. Fléchais, "Barry is not the weakest link: Eliciting secure system requirements with personas," *Proceedings of the 2010 24th BCS Interaction Specialist Group Conference (BCS-HCI'10)*, pp. 124–132, Sept. 2010.

[28] T. Adlin and J. Pruitt, *The Essential Persona Lifecycle: Your Guide to Building and Using Personas*. Morgan Kaufmann, 1st ed., 2010.

[29] L. Nielsen, "10 Steps to personas." `https://www.personas.dk/wp-content/uploads/2019/11/LOWRES-Personas-english-version-oktober-200821.pdf`, Oct. 2007. Last accessed 1st August 2020.

[30] L. Nielsen, *Personas — User Focused Design*. Springer, 2013.

[31] Tong Xin and Ban Xiaofang, "Online Banking Security Analysis based on STRIDE Threat Model," *International Journal of Security and Its Applications*, vol. 8, no. 2, pp. 271–282, 2014.

[32] M. Merhi, K. Hone, and A. Tarhini, "A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust," *Technology in Society*, vol. 59, pp. 101–151, 2019.

[33] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson, "Chip and Skim: Cloning EMV Cards with the Pre-play Attack," in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 49–64, May 2014.

[34] A. Hutchings, "Cambridge Computer Crime Database." `https://www.cl.cam.ac.uk/~ah793/cccd.html`. Last accessed 1st August 2020.

[35] British Computer Society (BCS), "Cybercrime Forensics Specialist Group Briefings." Compiled by Denis Edgar-Nevill (Canterbury Christ Church University), available via group distribution list, 2010–2014.

[36] Federal Bureau of Investigation (FBI), "Cyber's Most Wanted." `https://www.fbi.gov/wanted/cyber`, 2020. Last accessed 1st August 2020.

[37] GitHub, "VERIS Community Database." `https://github.com/vz-risk/VCDB`, 2020. Last accessed 1st August 2020.

[38] M. Volkamer and K. Renaud, *Number Theory and Cryptography*, ch. Mental Models – General Introduction and Review of Their Application to Human-Centred Security, pp. 255–280. Dec. 2013.

[39] M. R. Endsley and E. S. Connors, *Cyber Defense and Situational Awareness*, vol. 62 of *Advances in Information Security*, ch. Foundation and Challenges, pp. 7–27. Springer, 2014.

[40] A. Bruun, M. Larusdottir, L. Nielsen, P. Nielsen, and J. Persson, "The Role of UX Professionals in Agile Development: A Case Study From Industry," in *Proceedings of the 10th Nordic Conference on Computer-Human Interaction (NordiCHI'18)*, pp. 352–363, ACM, 2018.

[41] S. Bødker, E. Christiansen, T. Nyvang, and P.-O. Zander, "Personas, people and participation — Challenges from the trenches of local government," *Proceedings of the 12th Participatory Design Conference (PDC'12)*, vol. 1, pp. 91–100, Aug. 2012.

[42] C. Meyers, S. Powers, and D. Faissol, "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches," tech. rep., U.S. Department of Energy, Lawrence Livermore National Laboratory, Apr. 2009.

[43] M. K. Rogers, "Psychological theories of crime and hacking." `homes.cerias.purdue.edu/~mkr/crime.doc`, 2000. Last accessed 1st August 2020.

[44] A. Steele and X. Jia, "Adversary Centered Design: Threat Modeling Using Anti-Scenarios, Anti-Use Cases and Anti-Personas," in *Proceedings of the 2008 International Conference on Information and Knowledge Engineering (IKE'08)*, (Las Vegas, NV, US), pp. 367–370, CSREA Press, July 2008.

[45] M. Tariq, J. Brynielsson, and H. Artman, "Framing the Attacker in Organized Cybercrime," in *European Intelligence and Security Informatics Conference (EISIC'12)*, (Odense, Denmark), pp. 30–37, Aug. 2012.

[46] M. K. Rogers, "A new hacker taxonomy." `homes.cerias.purdue.edu/~mkr/hacker.doc`, 1999. Last accessed 1st August 2020.

[47] A. Altaf, S. Faily, H. Dogan, A. Mylonas, and E. Thron, "Identifying Safety and Human Factors Issues in Rail using IRIS and CAIRIS," in *Proceedings of the 5th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS'19)*, 2019.

[48] A. Alarifi, M. Alsaleh, and N. Alomar, "A model for evaluating the security and usability of e-banking platforms," *Computing*, vol. 99, pp. 519–535, 2017.

[49] T. Ngalo, H. Xiao, B. Christianson, and Y. Zhang, "Threat Analysis of Software Agents in Online Banking and Payments," in *16th Intl. Conf. on Dependable, Autonomic and Secure Computing, 16th Intl. Conf. on Pervasive Intelligence and Computing, 4th Intl. Conf. on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, pp. 716–723, IEEE, 2018.

[50] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in ebanking and the effects of experience," *Interacting with Computers*, vol. 22, pp. 153–164, May 2010.

[51] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers & Security*, vol. 30, no. 4, pp. 208–220, 2011.

[52] S. Alhumoud, L. Alabdulkarim, N. Almobarak, and A. Al-Wabil, "Socio-Cultural Aspects in the Design of Multilingual Banking Interfaces in the Arab Region," *Human-Computer Interaction: Users and Contexts*, pp. 269–280, 2015.

[53] C. Moeckel, "Human-computer interaction for security research: The case of EU e-banking systems," in *Human-Computer Interaction – INTERACT 2011* (P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque, and M. Winckler, eds.), pp. 406–409, Springer, 2011.

[54] C. Urquhart, H. Lehmann, and M. D. Myers, "Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems," *Information Systems*, vol. 20, no. 4, pp. 357–381, 2010.

[55] A. Shostack, "Who Are We Kidding with Attacker-Centered Threat Modeling?." `https://adam.shostack.org/blog/2019/10/who-are-we-kidding-with-attacker-centered-threat-modeling/`, Oct. 2019. Last accessed 1st August 2020.

[56] M. Wills, *The Official (ISC)2 SSCP CBK Reference*. Sybex/Wiley, 2020.

[57] I. Cervesato, "The Dolev-Yao Intruder is the Most Powerful Attacker," in *Proceedings of the 2001 16th Annual Symposium on Logic in Computer Science (LICS'01)*, pp. 16–19, IEEE, 2001.

[58] F. Shull and N. Mead, "Cyber threat modeling: An evaluation of three methods." `https://insights.sei.cmu.edu/sei_blog/2016/11/cyber-threat-modeling-an-evaluation-of-three-methods.html`, 2016. In Carnegie Mellon University Software Engineering Institute (SEI) Insights blog. Last accessed 1st August 2020.

[59] D. J. Ivoce, "Collaring the cybercrook: An investigator's view," *IEEE Spectrum*, vol. 34, pp. 31–36, June 1997.

[60] S. Faily and I. Fléchais, "The Secret Lives of Assumptions: Developing and Refining Assumption Personas for Secure System Design," in *Proceedings of the Third International Conference on Human-Centred Software Engineering (HCSE'10)*, vol. 6409 of *Lecture Notes in Computer Science*, (Reykjavik, Iceland), Springer, Oct. 2010.

[61] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering — A systematic literature review," *Information and Software Technology*, no. 51, pp. 7–15, 2008.

[62] K. Tuma, G. Calikli, and R. Scandariato, "Threat analysis of software systems: a systematic literature review," *Journal of Systems and Software*, vol. 144, pp. 275–294, 2018.

[63] S. Jalali and C. Wohlin, "Systematic Literature Studies: Database Searches vs. Backward Snowballing," in *2012 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM'12)*, (Lund, Sweden), Sept. 2012.

[64] S. D. Applegate and A. Stavrou, "Towards a Cyber Conflict Taxonomy," *Proceedings of the 2013 5th International Conference on Cyber Conflict (CYCON'13)*, 2013.

[65] R. Koelle, G. Markarian, and A. Tarter, *Aviation Security Engineering*. Artech House, 2011.

[66] X. Yuan, E. Nuakoh, I. Williams, and H. Yu, "Developing abuse cases based on threat modeling and attack patterns," *Journal of Software*, vol. 10, 2015.

[67] P. Schoo and R. Marx, "Threat Model Based Security Evaluation of Open Connectivity Services," in *International Conference on Mobile Networks and Management (MONAMI'12)*, vol. 58 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST)*, pp. 313–322, 2012.

[68] A. Padmos, "Against Mindset," in *Proceedings of the New Security Paradigms Workshop (NSPW'18)* (M. Carvalho, M. Bishop, A. Somayaji, W. Pieters, and M. Mannan, eds.), (Windsor, UK), pp. 12–27, ACM, Aug. 2018.

[69] S. Mauw and M. Oostdijk, "Foundations of attack trees," in *International Conference on Information Security and Cryptology (ICISC'05)*, vol. 3935 of *Lecture Notes in Computer Science book series (LNCS)*, pp. 186–198, Springer, 2005.

[70] P. Karpati, A. L. Opdahl, and G. Sindre, "HARM: Hacker Attack Representation Method," in *Proceedings of the 2010 5th International Conference on Software and Data Technologies (ICSOFT'10)*, (Athens, Greece), Springer, July 2010.

[71] D. Fraunholz, S. D. Anton, and H. D. Schotten, "Introducing GAMfIS: A generic attacker model for information security," *Proceedings of the 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM'17)*, pp. 1–6, 2017.

[72] M. Adams and M. Makramalla, "Cybersecurity skills training: An attacker-centric gamified approach," *Technology Innovation Management Review*, Jan. 2015.

[73] X. Peng and H. Zhao, "A Framework of Attacker Centric Cyber Attack Behavior Analysis," in *Proceedings of the 2010 5th International Conference on Software and Data Technologies (ICSOFT'10)*, (Athens, Greece), Springer, July 2010.

[74] T. Casey, P. Koeberl, and C. Vishik, "Threat Agents: A Necessary Component of Threat Analysis," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW'10)*, (New York, NY, USA), pp. 56:1–56:4, ACM, 2010.

[75] D. P. Mirembe and M. Muyeba, "Threat Modeling Revisited: Improving Expressiveness of Attack," in *Proceedings of the 2nd UKSIM European Symposium on Computer Modeling and Simulation*, (Liverpool, UK), IEEE, Sept. 2008.

[76] S. Paul and R. Vignon-Davillier, "Unifying traditional risk assessment approaches with attack trees," *Information Security and Applications*, vol. 19, pp. 165–181, July 2014.

[77] M. Morana and T. UcedaVélez, *Risk Centric Threat Modelling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons, 2015.

[78] M. Hollick, A. Perrig, C. Nita-Rotaru, P. Papadimitratos, and S. Schmid, "Toward a taxonomy and attacker model for secure routing protocols," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 1, 2017.

[79] B. Kordy, S. Mauw, S. Radomirovic, and P. Schweitzer, "Foundations of Attack-Defense Trees," in *Proceedings of the International Workshop on Formal Aspects in Security and Trust (FAST'10)*, vol. 6561 of *Lecture Notes in Computer Science (LNCS)*, pp. 80–95, Springer, 2010.

[80] B. Schneier, "Attack trees." `https://www.schneier.com/academic/archives/1999/12/attack_trees.html`, Dec. 1999. Last accessed 1st August 2020.

[81] H. Mantel and C. W. Probst, "On the Meaning and Purpose of Attack Trees," in *IEEE 32nd Computer Security Foundations Symposium (CSF'19)*, pp. 184–200, IEEE, 2019.

[82] S. De, M. S. Barik, and I. Banerjee, "Goal-Based Threat Modeling for Peer-to-Peer Cloud," *Procedia Computer Science*, vol. 89, pp. 64–72, 2016.

[83] M. Morana, "Threat Modeling Fundamentals and New PASTA Process, Application Threat Modelling Workshop (ISACA Ireland and OWASP Dublin)," Nov. 2013.

[84] H. Al-Mohannadi, I. Awan, and J. A. Hamar, "Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence," *Service Oriented Computing and Applications*, Jan. 2020.

[85] M. Rocchetto and N. O. Tippenhauer, "On Attacker Models and Profiles for Cyber-Physical Systems," in *Computer Security — ESORICS 2016* (I. Askoxylakis, S. Ioannidis, S. Katsikas, and C. Meadows, eds.), vol. 9879 of *Lecture Notes in Computer Science (LNCS)*, 2016.

[86] L. Othmane, R. Ranchal, R. Fernando, B. Bhargava, and E. Bodden, "Incorporating attacker capabilities in risk estimation and mitigation," *Computers and Security*, vol. 51, 2015.

[87] G. Bella, "The Rational Attacker." `http://www.dmi.unict.it/~giamp/Seminars/rationalattackerSAP08.pdf`, 2008. Invited talk at SAP Research France, Sophia Antipolis. Last accessed 1st August 2020.

[88] W. Arsac, G. Bella, X. Chantry, and L. Compagna, "Validating Security Protocols under the General Attacker," in *Foundations and Applications of Security Analysis* (P. Degano and L. Vigano, eds.), vol. 5511 of *Lecture Notes in Computer Science*, pp. 34–51, Springer, 2009.

[89] S. Li, R. Rickert, and A. Sliva, "Risk-Based Models of Attacker Behavior in Cybersecurity," in *Social Computing, Behavioral-Cultural Modeling and Prediction* (A. M. Greenberg, W. G. Kennedy, and N. D. Bos, eds.), vol. 7812 of *Lecture Notes in Computer Science (LNCS)*, pp. 523–532, Springer, 2013.

[90] Q. Do, B. Martini, and K.-K. R. Choo, "The role of the adversary model in applied security research," *Computers & Security*, vol. 81, pp. 156–181, Mar. 2019.

[91] K. J. Higgins, "Profiling the cybercriminal and the cyberspy." `http://www.darkreading.com/vulnerability/profiling-the-cybercriminal-and-the-cybe/240008081`, Sept. 2012. Dark Reading. Last accessed 1st August 2020.

[92] R. Leukfeldt, *Cybercriminal Networks*. Eleven International Publishing, 2016.

[93] R. Chiesa, S. Ducci, and S. Ciappi, *Profiling Hackers — The Science of Criminal Profiling as Applied to the World of Hacking*. Auerbach Publications, 2008.

[94] H. Thackray, "Hackers gonna hack, but do they know why? (DEFCON 25 SE Village)." `https://archive.org/details/youtube-TTx7mHzyX8c`, Oct. 2017. Last accessed 1st August 2020.

[95] P. H. Meland, D. G. Spampinato, E. Hagen, E. T. Baadshaug, K.-M. Krister, and K. S. Velle, "SeaMonster: Providing tool support for security modeling," *Norsk informasjonssikkerhetskonferanse (NISK'08)*, 2008.

[96] S. Faily, *Designing Usable and Secure Software with IRIS and CAIRIS*. Springer, 2018.

[97] I. A. Tøndel, T. Oyetoyan, M. Jaatun, and D. Cruzes, "Understanding challenges to adoption of the Microsoft elevation of privilege game," *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security (HoTSoS'18)*, vol. 2, pp. 1–10, Apr. 2018.

[98] P. Meland, I. Tøndel, and J. Jensen, "Idea: Reusability of Threat Models — Two Approaches with an Experimental Evaluation," in *Engineering Secure Software and Systems (ESSoS'10)* (F. M. F., D. Wallach, and N. Zannone, eds.), vol. 5965 of *Lecture Notes in Computer Science (LNCS)*, Springer, 2010.

[99] A. Shostack, "Threat modeling in 2018," *Black Hat USA*, 2018.

[100] R. Barnard, *Intrusion Detection Systems*. Gulf Professional Publishing, 1988.

[101] L. Kohnfelder and P. Garg, "The threats to our products." Via `https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx`, Apr. 1999. Last accessed 1st August 2020.

[102] F. Swiderski and W. Snyder, *Threat Modeling*. Microsoft Professional, 2004.

[103] C. Slater, O. S. Saydjari, B. Schneier, and J. Wallner, "Toward a Secure System Engineering Methodolgy," in *Proceedings of the 1998 Workshop on New Security Paradigms* (B. Blakley, D. M. Kienzle, M. E. Zurko, and S. J. Greenwald, eds.), (Charlottsville, VA, USA), pp. 2–10, ACM, Sept. 1998.

[104] M. Goodwin, "Real-World Threat Modelling." `https://medium.com/sagefuturemakers/real-world-threat-modelling-fb14ef767c49`, Jan. 2020. Sage Developer Blog. Last accessed 1st August 2020.

[105] M. Lewis, "Tackling 5G security with threat modelling." `https://www.nccgroup.com/uk/about-us/newsroom-and-events/blogs/2018/march/tackling-5g-security-with-threat-modelling/`, Mar. 2018. NCC Group blog. Last accessed 1st August 2020.

[106] ThreatModeler, "Product website." `https://threatmodeler.com/`, 2020. Last accessed 1st August 2020.

[107] W. Xiong and R. Lagerström, "Threat modeling — A systematic literature review," *Computers & security*, vol. 84, pp. 53–59, 2019.

[108] T. Williams and L. Cavallaro, "The Value of Threat Modelling." `https://www.computerweekly.com/ehandbook/The-Value-of-Threat-Modelling`, Mar. 2016. Royal Holloway information security thesis series. ComputerWeekly special report.

[109] R. Scandariato, K. Wuyts, and W. Joosen, "A descriptive study of Microsoft's threat modeling technique," *Requirements Engineering*, vol. 20, pp. 163–180, 2015.

[110] C. Moeckel and A. E. Abdallah, "Understanding the Value and Potential of Threat Modeling for Application Security Design — An E-Banking Case Study," *Journal of Information Assurance and Security*, vol. 6, no. 5, pp. 346–356, 2011.

[111] L. O. Nweke and S. Wolthusen, "A Review of Asset-Centric Threat Modelling Approaches," *International Journal of Advanced Computer Science and Applications*, vol. 11, pp. 1–6, Mar. 2020.

[112] K. Bernsmed and M. G. Jaatun, "Threat modelling and agile software development: Identified practice in four Norwegian organisations," in *2019 International Conference on Cyber Security and Protection of Digital Services*, (Oxford, UK), pp. 1–8, June 2019.

[113] Microsoft, "Secure Development Documentation: Microsoft Threat Modeling Tool." `https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool`, Feb. 2017. Last accessed 1st August 2020.

[114] A. Shostack, "Modeling Attackers and Their Motives." `https://adam.shostack.org/blog/2014/11/modeling-attackers-and-their-motives/`, Nov. 2014. Last accessed 1st August 2020.

[115] T. Martin-Vegue, "How to Improve Your Risk Assessments with Attacker-Centric Threat Modeling." Available via `https://www.slideshare.net/tonymartinvegue/how-to-improve-your-risk-assessments-with-attackercentric-threat-modeling`, 2014. ISACA San Francisco Chapter: 2014 Fall Conference. Last accessed 1st August 2020.

[116] J. Cleland-Huang, "How Well Do You Know Your Personae Non Gratae?," *IEEE Software*, pp. 28–31, July 2014.

[117] T. Denning, B. Friedman, and T. Kohno, "The Security Cards — a Security Threat Brainstorming Toolkit." http://securitycards.cs.washington.edu, 2013. Last accessed 1st August 2020.

[118] OWASP Open Security Summit, "State and Future of Threat Modeling." https://2019.open-security-summit.org/outcomes/threat-modeling/working-sessions/future-of-threat-modelling/, June 2019. Last accessed 1st August 2020.

[119] Lock Heed Martin Corporation, "Gaining the advantage — Applying cyber kill chain methodology to network defense." https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf, 2018. Last accessed 1st August 2020.

[120] J. Brynielsson, U. Franke, M. Adnan Tariq, and S. Varga, "Using cyber defense exercises to obtain additional data for attacker profiling," in *Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI'16)*, pp. 37–42, 2016.

[121] UC Davis Website, "UC Davis Continuing and Professional Education: Cyber Security." https://cpe.ucdavis.edu/subject-areas/cybersecurity, 2020. Last accessed 1st August 2020.

[122] F. Katz, "Adversarial Thinking: Teaching Students to Think Like a Hacker," in *KSU Proceedings on Cybersecurity Education, Research and Practice*, no. 1, (https://digitalcommons.kennesaw.edu/ccerp/2019/education/1), Oct. 2019.

[123] S. T. Hamman and K. M. Hopkinson, "Teaching Adversarial Thinking for Cybersecurity," *Journal of the Colloquium for Information System Security Education (CISSE)*, Sept. 2016.

[124] F. B. Schneider, "Cybersecurity education in universities," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 3–4, 2013.

[125] M. Dark, "Thinking about Cybersecurity," *IEEE Security & Privacy*, pp. 61–65, Jan. 2015.

[126] S. L. Pfleeger, "DRAFT Report on the NIST Workshop (Usable Security)." http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.357.5862&rep=rep1&type=pdf, Aug. 2011. Last accessed 1st August 2020.

[127] A. Burnis, "Think Like an Attacker and Improve Your Defensive Strategy." https://www.cyberark.com/resources/blog/think-like-an-attacker-and-improve-your-defensive-strategy, May 2017. Last accessed 1st August 2020.

[128] I. Valenzuela, "How Thinking Like an Attacker Makes You a Better Threat Hunter." https://www.mcafee.com/blogs/enterprise/how-thinking-like-an-attacker-makes-a-better-threat-hunter/, Sept. 2017. Last accessed 1st August 2020.

[129] D. Palmer, "The best cyberdefence: Think like an attacker." https://www.zdnet.com/article/why-the-best-cyberdefence-is-to-think-like-an-attacker/, Apr. 2016. ZDNet. Last accessed 1st August 2020.

[130] M. Miller, "Drinks and Persona Building: Creating Adversary Trading Cards." https://open-security-summit.org/training/week-1/social/drinks-and-persona-building-creating-adversary-trading/, June 2020. OWASP Open Security Summit Trainings. Last accessed 1st August 2020.

[131] T. Chothia and J. de Ruiter, "Learning From Others' Mistakes: Penetrating Testing IoT Devices in the Classroom," in *25th Usenix Security Symposium — USENIX Workshop on Advances in Security Education (ASE'16)*, (https://www.usenix.org/system/files/conference/ase16/ase16-paper-chothia.pdf), pp. 1–8, 2016.

[132] N. Nykodym, R. Taylor, and J. Vilela, "Criminal profiling and insider cyber crime," *Digital Investigation*, vol. 2, no. 4, pp. 261–267, 2005.

[133] S. Gordon, "The generic virus writer I+II," in *6th International Virus Bulletin Conference, Brighton, UK*, September 1996.

[134] R. C. Hollinger, "Computer hackers follow a guttman-like progression," *Phrack Inc.*, vol. 2, April 1988.

[135] W. Landreth, *Out of the Inner Circle: A Hacker's Guide to Computer Security*. Microsoft Press, 1989.

[136] C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, *Security in Computing*. Prentice Hall, 5th ed., 2015.

[137] C. P. Pfleeger, *Security in Computing*. Prentice Hall, 2nd ed., 1997.

[138] A. Chandler, "The changing definition and image of hackers in popular discourse," *International Journal of the Sociology of Law, Elsevier*, vol. 24, no. 2, pp. 229–251, 1996.

[139] M. Kilger, O. Arkin, and J. Sutzman, *Know Your Enemy — Learning About Security Threats*, ch. Profiling, pp. 503–556. Addison-Wesley, 2004.

[140] W. Ziegler and C. S. Fötinger, "Understanding a hacker's mind — a psychological insight into the hijacking of identities," 2004. White Paper by the Danube University Krems (Austria) and RSA Security.

[141] R. Borges Da Silva, "Taxonomy and typology: are they really synonymous?," *Sante Publique*, vol. 25, no. 5, pp. 633–637, 2013.

[142] K. D. Bailey, *Typologies and Taxonomies: An Introduction to Classification Techniques*. SAGE Publications, 1994.

[143] L. A. Long and E. Hadsell, "Profiling Hackers." `http://www.sans.org/reading_room/whitepapers/hackers/profiling-hackers_33864`, January 2012. SANS Institute InfoSec Reading Room. Last accessed 1st August 2020.

[144] T. Parker, E. Shaw, E. Stroz, M. G. Devost, and M. H. Sachs, *Cyber Adversary Characterisation — Auditing the Hacker Mind*. Syngress, 2004.

[145] E. Chabrow, "7 Levels of hackers — Applying an ancient Chinese lesson: know your enemies." `http://www.govinfosecurity.com/blogs.php?postID=1206`, Feb. 2012. GovInfoSecurity. Last accessed 1st August 2020.

[146] Z. Xu, Q. Hu, and C. Zhang, "Why computer talents become computer hackers," *Communications of the ACM*, vol. 56, pp. 64–74, Apr. 2013.

[147] L. Turner, "Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and Paypal." `https://www.independent.co.uk/news/uk/crime/anonymous-hackers-jailed-for-ddos-attacks-on-visa-mastercard-and-paypal-8465791.html`, Jan. 2013. The Independent. Last accessed 1st August 2020.

[148] Chaos Computer Club, "Chaos Computer Club analyzes government malware." `https://www.ccc.de/en/updates/2011/staatstrojaner`, Oct. 2011. Last accessed 1st August 2020.

[149] J. Kaiman, "China calls Australian spy HQ plans hacking claims 'groundless'." `http://www.guardian.co.uk/world/2013/may/28/china-asio-australian-spy-hq-hacking-claims`, May 2013. In The Guardian. Last accessed 1st August 2020.

[150] R. Hutton and N. Syeed, "Russia steps up hacking, spurring US–UK Warning on Risk." `https://www.bloomberg.com/news/articles/2018-04-16/u-s-and-u-k-issue-joint-alert-warning-of-russian-cyber-attacks`, Apr. 2018. Bloomberg. Last accessed 1st August 2020.

[151] D. J.-J. Robichaud, *Plato's Persona: Marsilio Ficino, Renaissance Humanism, and Platonic Traditions*, ch. Prosopon/Persona: Philosophy and Rhetoric, pp. 25–68. University of Pennsylvania Press, 2018.

[152] A. Canossa and A. Drachen, "Play-Personas: Behaviours and Belief Systems in User-Centred Game Design," in *INTERACT '09: Proceedings of the 12th IFIP TC 13 International Conference on Human-Computer Interaction: Part II* (T. Gross, J. Gulliksen, P. Kotzé, L. Oestreicher, P. Palanque, R. O. Prates, and M. Winckler, eds.), pp. 510–523, Springer, Aug. 2009.

[153] S. Serpa, "Ideal type in sociological research," *Sociology International Journal*, vol. 2, pp. 398–399, Sept. 2018.

[154] R. Swedberg, "How to use Max Weber's ideal type in sociological analysis," *Journal of Classical Sociology*, vol. 18, no. 3, pp. 181–196, 2018.

[155] D. Saunders, *Anti-Lawyers: Religion and the Critics of Law and State: Critics of Law as Heirs of Religion*. Routledge, 1997.

[156] P. du Gay, *Organizing Identity: Persons and Organizations after theory (Culture, Representation and Identity series)*. SAGE Publications, 2007.

[157] A. Cooper, *The Inmates Are Running the Asylum*. Macmillan UK, 1999.

[158] D. Norman, "Ad-Hoc Personas & Empathetic Focus." https://jnd.org/ad-hoc_personas_empathetic_focus, Nov. 2004. Last accessed 1st August 2020.

[159] A. Dix, J. Finlay, G. D. Abowd, and R. Beale, *Human-Computer Interaction*. Prentice Hall, Upper Saddle River, NJ, US, 3rd ed., 2004.

[160] P. Bagnall, "Using personas effectively," in *Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction (BCS HCI 2008)*, vol. 2, (Liverpool, UK), pp. 215–216, British Computer Society (BCS), Sept. 2008.

[161] H. Sharp, Y. Rogers, and J. Preece, *Interaction Design — Beyond Human-Computer Interaction*. John Wiley & Sons, UK, 2nd ed., 2007.

[162] P. Turner and S. Turner, "Is stereotyping inevitable when designing with personas?," *Design Studies*, vol. 32, pp. 30–44, 2011.

[163] T. Matthews, T. Judge, and S. Whittaker, "How do designers and user experience professionals actually perceive and use personas?," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'12)*, (Austin, TX, US), pp. 1219–1228, ACM, May 2012.

[164] A. Blomquist and M. Arvola, "Personas in action: Ethnography in an interaction design team," in *Proceedings of the Second Nordic Conference on Human-Computer Interaction (NordiCHI'02)*, (Aarhus, Denmark), pp. 197–200, ACM, Oct. 2002.

[165] J.-L. W. Dupree, E. Lank, and D. M. Berry, "A case study of using grounded analysis as a requirement engineering method: Identifying personas that specify privacy and security tool users," *Science of Computer Programming*, vol. 152, p. 1, Jan. 2018.

[166] S. Faily and I. Fléchais, "Persona Cases: A Technique for Grounding Personas," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'11)*, pp. 2267–2270, ACM, 2011.

[167] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Computers & Security, Elsevier*, vol. 70, pp. p.663–674, Sept. 2017.

[168] L. Bell, M. Brunton-Spall, R. Smith, and J. Bird, *Agile Application Security: Enabling Security in a Continuous Delivery Pipeline*. O'Reilly Media, 2017.

[169] R. Oldham and P. Huggins, "Threat personas and application vulnerability scoring model." https://open-security-summit.org/tracks/ciso-and-risk-management/user-sessions/threat-personas-and-application-vulnerability-management/, June 2020. Last accessed 1st August 2020.

[170] B. Glaser and J. Holton, "Remodeling Grounded Theory," *Forum Qualitative Sozialforschung*, vol. 5, no. 2, 2004.

[171] T. Olanrewaju, "The rise of the digital bank." https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-rise-of-the-digital-bank, July 2014. McKinsey & Company (Digital McKinsey). Last accessed 1st August 2020.

[172] U. Gasser, O. Gassmann, T. Hens, L. Leifer, T. Puschmann, and L. Zhao, "Digital banking 2025." https://www.alexandria.unisg.ch/253962, 2017. Last accessed 1st August 2020.

[173] C. I. Mbama and P. O. Ezepue, "Digital banking, customer experience and bank financial performance: UK customers' perceptions," *International Journal of Bank Marketing*, vol. 36, no. 2, pp. 230–255, 2018.

[174] A. Larsson and Y. Viitaoja, "Building customer loyalty in digital banking: A study of bank staff's perspectives on the challenges of digital CRM and loyalty," *International Journal of Bank Marketing*, vol. 35, no. 6, pp. 858–877, 2017.

[175] J. Ginovsky, "What really is 'digital banking'?." Available via https://web.archive.org/web/20190714163910/http://www.bankingexchange.com/blogs-3/making-sense-of-it-all/item/5187-what-really-is-digital-banking, Apr. 2015. In Banking Exchange. Last accessed 1st August 2020.

[176] S. Epstein, "Understanding Digital Banking." https://www.finextra.com/blogposting/10390/understanding-digital-banking, 2015. In FinExtra. Last accessed 1st August 2020.

[177] Z. Bareisis and D. Latimore, "Defining a digital financial institution: What 'digital' means in banking." https://www.celent.com/insights/268657967, Dec. 2014. Celent Consulting. Last accessed 1st August 2020.

[178] PricewaterhouseCoopers LLP (PwC), "The new digital tipping point." `https://preview.thenewsmarket.com/Previews/PWC/DocumentAssets/225502.pdf`, 2011. Last accessed 1st August 2020.

[179] A. Lipton, D. Shrier, and A. Pentland, "Digital Banking Manifesto: The End of Banks?." `https://globalriskinstitute.org/publications/digital-banking-manifesto-the-end-of-banks`, 2016. Global Risk Institute & Massachusetts Institute of Technology. Last accessed 1st August 2020.

[180] C. H. Winnefeld and A. Permantier, "FinTech — The digital (R)Evolution in the German Banking Sector?," *Business and Management Research*, vol. 6, no. 3, pp. 65–84, 2017.

[181] G. Dorfleitner, L. Hornuf, M. Schmitt, and M. Weber, *FinTech in Germany*, ch. Definition of FinTech and Description of the FinTech Industry, pp. 5–10. Springer, 2017.

[182] J. Kaye, J. Vertesi, J. Ferreira, B. Brown, and M. Perry, "#CHIMoney: Financial Interactions, Digital Cash, Capital Exchange and Mobile Money," in *CHI '14 Extended Abstracts on Human Factors in Computing Systems (CHI EA'14)*, pp. 111–114, ACM, Apr. 2014.

[183] J. Kaye, M. McCuistion, R. Gulotta, and D. A. Shamma, "Money talks: tracking personal finances," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'14)*, pp. 521–530, ACM, 2014.

[184] M. Lewis and M. Perry, "Follow the Money: Managing Personal Finance," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI'19)*, ACM, May 2019.

[185] M. Perry and J. Ferreira, "Moneywork: Practices of Use and Social Interaction around Digital and Analog Money," in *Transactions on Computer-Human Interaction*, vol. 24, pp. 41:1–41:33, ACM, Jan. 2018.

[186] N. Fierro and C. Zapata, "Usability Heuristics for Web Banking," in *Design, User Experience, and Usability: Design Thinking and Methods (DUXU 2016)* (A. Marcus, ed.), vol. 9746 of *Lecture Notes in Computer Science (LNCS)*, pp. 412–423, Springer, 2016.

[187] M. Hertzum, N. Jørgensen, and M. Nørgaard, "Usable security and e-banking: Ease of use vis-à-vis security," *Australasian Journal of Information Systems (Special Issue)*, vol. 11, pp. 52–65, Apr. 2004.

[188] A. Whitten and J. Tygar, "Why Johnny can't encrypt: a usability evaluation of PGP 5.0," in *Proceedings of the 8th USENIX Security Symposium (USENIX'99)*, (Berkeley, CA, US), 1999.

[189] S. Furnell, "A comparison of website user authentication mechanisms," *Computer Fraud & Security*, pp. 5–9, Sept. 2007.

[190] C. Braz, A. Seffah, and D. M'Raihi, "Designing a Trade-Off Between Usability and Security: A Metrics Based-Model," in *Human-Computer Interaction – INTERACT 2007* (C. Baranauskas, P. Palanque, J. Abascal, and S. D. J. Barbosa, eds.), vol. 4663 of *Lecture Notes in Computer Science (LNCS)*, pp. 114–126, Springer, 2007.

[191] M. Mannan and P. C. van Oorschot, "Security and usability: the gap in real-world online banking," in *NSPW '07: Proceedings of the 2007 Workshop on New Security Paradigms*, pp. 1–14, July 2008.

[192] L. F. Cranor and S. Garfinkel, *Security and Usability*. O'Reilly, 2005.

[193] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[194] T. Pikkarainen, K. Pikkarainen, H. Karjaluoto, and S. Pahnila, "Consumer acceptance of online banking: an extension of the technology acceptance model," *Internet Research*, vol. 14, no. 3, pp. 224–235, 2004.

[195] M. Nilsson, A. Adams, and S. Herd, "Building security and trust in online banking," in *CHI '05 Extended Abstracts on Human Factors in Computing Systems (CHI EA'05)*, pp. 1701–1704, ACM, 2005.

[196] S. Drimer, S. J. Murdoch, and R. Anderson, "Optimised to Fail: Card Readers for Online Banking," in *Financial Cryptography and Data Security* (R. Dingledine and P. Golle, eds.), no. 5628 in Lecture Notes in Computer Science (LNCS), pp. 184–200, Springer, 2009.

[197] S. Kiljan, K. Simoens, D. D. Cock, M. van Eekelen, and H. Vranken, "A Survey of Authentication and Communications Security in Online Banking," *ACM Computing Surveys*, vol. 49, pp. 61:1–61:35, Dec. 2016.

[198] J. Choubey and B. Choubey, "Secure User Authentication in Internet Banking: A Qualitative Survey," *International Journal of Innovation, Management and Technology*, vol. 4, pp. 198–203, Apr. 2013.

[199] F. Sinigaglia, R. Carbone, G. Costac, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild," *Computer & Security*, vol. 95, 2020.

[200] M. Just and D. Aspinall, "On the security and usability of dual credential authentication in UK online banking," in *Proceedings of the 2012 International Conference for Internet Technology And Secured Transactions (ICITST'12)*, pp. 259–264, IEEE, 2012.

[201] K. Krol, E. Philippou, E. Cristofaro, and M. Sasse, "'They brought in the horrible key ring thing!' Analysing the Usability of Two-Factor Authentication in UK Online Banking," in *Network and Distributed System Security (NDSS) Symposium: Workshop on Usable Security (USEC'15)*, (San Diego, CA, US), pp. 1–10, Internet Society, Feb. 2015.

[202] A. Svilar and J. Zupančič, "User Experience with Security Elements in Internet and Mobile Banking," *Organizacija, Volume 49*, vol. 49, pp. 251–260, Nov. 2016.

[203] K. Reese, T. Smith, J. Dutson, J. Armknecht, and J. Cameron, "A Usability Study of Five Two-Factor Authentication Methods," in *15th Symposium on Usable Privacy and Security (SOUPS'19)*, (Santa Clara, CA, US), USENIX Association, Aug. 2019.

[204] V. Zimmermann and N. Gerber, "The password is dead, long live the password — A laboratory study on user perceptions of authentication schemes," *International Journal of Human-Computer Studies*, vol. 133, pp. 26–44, Jan. 2020.

[205] E. D. Cristofaro, H. Du, J. Freudiger, and G. Norcie, "A Comparative Usability Study of Two-Factor Authentication," in *Network and Distributed System Security (NDSS) Symposium: Workshop on Usable Security (USEC'14)*, (San Diego, CA, US), Internet Society, 2014.

[206] Financial Ombudsman Service (UK), "For businesses: Complaints we deal with (fraud and scams)." `https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams`, June 2020. Last accessed 1st August 2020.

[207] Authorised Push Payments Scams Steering Group (UK), "APP Scams Steering Group Agrees Voluntary Code." `https://appcrmsteeringgroup.uk/app-scams-steering-group-agrees-voluntary-code`, Feb. 2019. Last accessed 1st August 2020.

[208] L. Warwick-Ching, "TSB fraud refund guarantee — what will it mean for victims?." `https://www.ft.com/content/d2134474-6115-11e9-a27a-fdd51850994c`, Apr. 2019. In Financial Times (UK). Last accessed 1st August 2020.

[209] K. Peachey, "Scam victims to be refunded by banks." `https://www.bbc.co.uk/news/business-48385426`, May 2019. In BBC News. Last accessed 1st August 2020.

[210] Monzo Bank Ltd (UK), "Stay safe with Monzo." `https://monzo.com/i/security`, 2020. Last accessed 1st August 2020.

[211] Barclays Bank UK, "Digital Eagles — Build your digital skills with us." `https://www.barclays.co.uk/digital-confidence/eagles`, 2020. Last accessed 1st August 2020.

[212] UK Finance, "Take five to stop fraud (campaign website)." `https://takefive-stopfraud.org.uk`. Last accessed 1st August 2020.

[213] UK Finance & Cifas, "Don't be Fooled (campaign website against money mule recruitment)." `https://www.moneymules.co.uk/index.html`, 2020. Last accessed 1st August 2020.

[214] I. Kirlappos and M. A. Sasse, "Security Education against Phishing: A Modest Proposal for a Major Rethink," *IEEE Security & Privacy*, vol. 10, pp. 24–32, Mar. 2012.

[215] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny Not to Fall for Phish," *ACM Transactions on Internet Technology*, vol. 10, p. 7, June 2010.

[216] J. Jansen and R. Leukfeldt, "Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization," *International Journal of Cyber Criminology*, vol. 10, pp. 79–92, Jan. 2016.

[217] M. Volkamer, K. Renaud, B. M. Reinheimer, P. Rack, M. Ghiglieri, P. Mayer, A. Kunz, and N. Gerber, "Developing and Evaluating a Five Minute Phishing Awareness Video," in *Proceedings of the 15th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2018)* (S. Furnell, ed.), vol. 11033 of *Security and Cryptology*, (Regensburg, Germany), pp. 119–134, Springer, Sept. 2018.

[218] B. K. Payne, *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, ch. Defining Cybercrime. Palgrave Macmillan, 2019.

[219] UK Crown Prosecution Service (CPS), "Victims of Crime (The Code of Practice) — CPS Legal Guidance." `https://www.cps.gov.uk/legal-guidance/victims-crime-code-practice-cps-legal-guidance`, 2017. Last accessed 1st August 2020.

[220] J. Lusthaus, *Industry of Anonymity*. Harvard University Press, 2018.

[221] E. Kraemer-Mbula, P. Tang, and H. Rush, "The Cybercrime Ecosystem: Online Innovation in the Shadows?," *Technological Forecasting and Social Change*, vol. 80, no. 3, pp. 541–555, 2013.

[222] A. K. Sood, R. Bansal, and R. J. Enbody, "Cybercrime: Dissecting the State of Underground Enterprise," *IEEE Internet Computing*, pp. 60–68, Jan. 2013. Cybercrimes Track.

[223] M. S. Keman Huang and S. Madnick, "Systematically Understanding the Cyber Attack Business: A Survey," *ACM Computing Surveys*, vol. 51, pp. 70:1–70:36, July 2018.

[224] J. R. C. Nurse and M. Bada, *The Oxford Handbook of Cyberpsychology*, ch. The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations. Oxford University Press, 2019.

[225] T. Moore, R. Clayton, and R. Anderson, "The Economics of Online Crime," *Journal of Economic Perspectives*, vol. 23, no. 3, pp. 3–20, 2009.

[226] J. Lusthaus, "How organised is organised cybercrime?," *Global Crime*, vol. 14, no. 1, pp. 52–60, 2013.

[227] K. Choo and R. Smith, "Criminal Exploitation of Online Systems by Organised Crime Groups," *Asian Journal of Criminology*, vol. 3, no. 1, pp. 37–59, 2008.

[228] A. Hutchings, "Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission," *Crime, Law and Social Change*, vol. 62, pp. 1–20, 2014.

[229] K.-K. R. Choo, "Organised crime groups in cyberspace: a typology," *Trends in Organised Crime*, vol. 11, pp. 270–295, July 2008.

[230] E. R. Leukfeldt, A. Lavorgna, and E. R. Kleemans, "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime," *European Journal on Criminal Policy and Research*, vol. 23, pp. 287–300, 2017.

[231] A. Lavorgna and A. Sergi, "Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom," *International Journal of Cyber Criminology (IJCC)*, vol. 10, no. 2, pp. 170–187, 2016.

[232] D. S. Wall, "Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime," *The European Review of Organised Crime*, vol. 2, no. 2, pp. 71–90, 2015.

[233] R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime," *International Journal of Cyber Criminology*, vol. 8, pp. 1–20, Jan. 2014.

[234] R. Thomas and J. Martin, "Team Cyrmru — The Underground Economy: Priceless," *; LOGIN:*, vol. 31, pp. 7–16, Dec. 2006.

[235] UK National Cyber Security Centre (NCSC), "Cyber crime: understanding the online business model." `https://www.ncsc.gov.uk/files/Cybercrime-understabndingtheonlinebusinessmodel.pdf`, 2017. Last accessed 1st August 2020.

[236] M. R. J. Soudijn and B. C. H. T. Zegers, "Cybercrime and virtual offender convergence settings," *Trends in Organized Crime*, vol. 15, pp. 111–129, Sept. 2012.

[237] S. R. Chabinsky, "The Cyber Threat: Who's Doing What to Whom? (Speech)." `https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom`, Mar. 2010. Deputy Assistant Director, Cyber Division Federal Bureau of Investigation (FBI). GovSec/FOSE Conference, Washington, D.C. Last accessed 1st August 2020.

[238] D. Birk, S. Gajek, F. Gröbert, and A.-R. Sadeghi, "Phishing Phishers — Observing and Tracing Organized Cybercrime," in *Proceedings of the 2nd International Conference on Internet Monitoring and Protection (ICIMP'07)*, 2007.

[239] J. Lusthaus and F. Varese, "Offline and local: The hidden face of cybercrime," *Policing: A Journal of Policy and Practice*, 2017.

[240] B. H. M. Custers, R. L. D. Pool, and R. Cornelisse, "Banking malware and the laundering of its profits," *European Journal of Criminology*, vol. 16, no. 6, pp. 728–745, 2019.

[241] M. S. Raza, Q. Zhan, and S. Rubab, "Role of money mules in money laundering and financial crimes a discussion through case studies," *Journal of Financial Crime*, May 2020.

[242] B. Krebs, "'Money Mule' Gangs Turn to Bitcoin ATMs." `https://krebsonsecurity.com/2016/09/money-mule-gangs-turn-to-bitcoin-atms`, Sept. 2016. Krebs on Security. Last accessed 1st August 2020.

[243] E. Leukfeldt and E. Kleemans, *Criminal Networks and Law Enforcement: Global Perspectives on Illegal Enterprise*, ch. Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms, pp. 75–89. Routledge, 2019.

[244] M. Aston, S. McCombie, B. Reardon, and P. Watters, "A Preliminary Profiling of Internet Money Mules: An Australian Perspective," in *Proceedings of 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*, (Brisbane, Australia), IEEE, 2009.

[245] R. Leukfeldt and J. Jansen, "Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands," *International Journal of Cyber Criminology*, vol. 9, pp. 173–184, Dec. 2015.

[246] B. Krebs, "Coronavirus Widens the Money Mule Pool." `https://krebsonsecurity.com/2020/03/coronavirus-widens-the-money-mule-pool`, Mar. 2020. Krebs on Security. Last accessed 1st August 2020.

[247] L. F. Cranor, "Can Phishing Be Foiled?," *Scientific American: Computer Security*, pp. 104–110, Dec. 2008.

[248] A. Mikhaylov and R. Frank, "Cards, Money and Two Hacking Forums — An Analysis of Online Money Laundering Schemes," in *Proceedings of the 2016 European Intelligence and Security Informatics Conference (EISIC'16)*, (Uppsala, Sweden), pp. 80–83, IEEE, Aug. 2016.

[249] Cifas (UK), "Fraudscape: Identity Fraud and Money Mules Rise Again." `https://www.cifas.org.uk/insight/reports-trends/fraudscape-2019`, 2019. Report. Last accessed 1st August 2020.

[250] J. Saldaña, "Researcher, Analyze Thyself," *International Journal of Qualitative Methods*, vol. 17, no. 1, 2018.

[251] J. W. Creswell, *Research Design (International Student Edition): Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications, 2013.

[252] E. S. Guba and Y. S. Lincoln, *Handbook of Qualitative Research*, ch. Competing Paradigms in Qualitative Research, pp. 105–117. SAGE Publications, 1994.

[253] K. Charmaz, *Constructing Grounded Theory*. SAGE Publications, 2nd ed., 2014.

[254] C. Urquhart, *Grounded Theory for Qualitative Research*. SAGE Publications, 1st edition ed., 2013.

[255] M. Muller and S. Kogan, *The Human Computer Interaction Handbook*, ch. Grounded Theory Method in Human-Computer Interaction and Computer-Supported Cooperative Work, pp. 1003–1049. CRC Press (Taylor & Francis), 3rd ed., 2012.

[256] V. Timonen, G. Foley, and C. Conlon, "Challenges When Using Grounded Theory: A Pragmatic Introduction to Doing GT Research," *International Journal of Qualitative Methods*, vol. 17, no. 1, 2018.

[257] J. C. Hood, *The SAGE Handbook of Grounded Theory*, ch. Orthodoxy vs. Power: The Defining Traits of Grounded Theory, pp. 151–164. SAGE Publications, 2007.

[258] A. E. Clarke and C. Friese, *The SAGE Handbook of Grounded Theory*, ch. Grounded Theorizing Using Situational Analysis, pp. 363–397. SAGE Publications, 2007.

[259] D. R. Thomas, "A General Inductive Approach for Analyzing Qualitative Evaluation Data," *American Journal of Evaluation*, vol. 27, no. 2, pp. 237–246, 2006.

[260] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, pp. 40–46, Dec. 1999.

[261] V. Kaptelinin, B. Nardi, S. Bødker, J. Carroll, J. Hollan, E. Hutchins, and T. Winograd, "Post-cognitivist HCI: second-wave theories," in *CHI '03 Extended Abstracts on Human Factors in Computing Systems (CHI EA'03)*, pp. 692–693, ACM, Apr. 2003.

[262] D. Furniss, A. Blandford, and P. Curzon, "Confessions from a Grounded Theory PhD: Experiences and Lessons Learnt," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'11)*, pp. 113–122, ACM, 2011.

[263] A. Adams, P. Lunt, and P. Cairns, *Research Methods for Human-Computer Interaction*, ch. A qualitiative approach to HCI research, pp. pp. 138–157. Cambridge University Press, 2008.

[264] Olga Hörding, Mady Torres de Souza, and Sohit Karol, "The Story of Spotify Personas." `https://spotify.design/article/the-story-of-spotify-personas`, Mar. 2019. Last accessed 1st August 2020.

[265] C. Willig, *Introducing Qualitative Research in Psychology — Adventures in Theory and Method*, ch. Grounded theory, pp. 34–51. Open University Press – McGraw-Hill Education, 2008.

[266] E. Hollywell, *Genuinely caring: compassion and the healing nature of the therapeutic relationship*. PhD thesis, City University London, `https://openaccess.city.ac.uk/id/eprint/14549/`, 2015. Last accessed 1st August 2020.

[267] M. Whiteside, J. Mills, and J. McCalman, "Using secondary data for grounded theory analysis," *Australian Social Work*, vol. 65, no. 4, pp. 504–516, 2012.

[268] L. Andrews, A. Higgins, M. Waring, and J. Lalor, "Using Classic Grounded Theory to analyse secondary data: reality and reflections," *Grounded Theory Review*, vol. 11, pp. 12–26, Dec. 2012.

[269] K. S. Taber, "Grounded Theory: A Research Methodology." Workshop at University of Cambridge, November 2013.

[270] A. Bryant and K. Charmaz, *The SAGE Handbook of Grounded Theory*. SAGE Publications, 2007.

[271] J. Saldaña, *The Coding Manual for Qualitative Researchers*. SAGE Publications, 2nd edition ed., 2012.

[272] B. Glaser, *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*. Sociology Press, 1978.

[273] K. S. Taber, *School-based Research: A Guide for Education Students*, ch. Building theory from data: grounded theory, pp. 216–229. SAGE Publications, 2009.

[274] A. L. Strauss and J. M. Corbin, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. SAGE Publications, 2nd ed., 1998.

[275] C. Moeckel, "Examining and Constructing Attacker Categorisations: an Experimental Typology for Digital Banking," *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19): 1st International Workshop on Information Security Methodology and Replication Studies (IWSMR 2019)*, vol. 93, 2019. ACM.

[276] C. Moeckel, "(De-)Constructing Attacker Categorisations: A Typology Iteration for the Case of Digital Banking," *Journal of Universal Computer Science (J.UCS) — Special Issue on Information Security Methodology, Replication Studies and Information Security Education*, Nov. 2020 *(forthcoming)*.

[277] S. Bødker and C. N. Klokmose, "From persona to techsona," in *Human-Computer Interaction – INTERACT 2013* (P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson, and M. Winckler, eds.), vol. 8120 of *Lecture Notes in Computer Science (LNCS)*, pp. 342–349, Springer, 2013.

[278] A. Cooper, R. Reimann, and D. Cronin, *About Face 3 — The Essentials of Interaction Design*. Wiley Publishing, 2007.

[279] J. Grudin and J. Pruitt, "Personas, Participatory Design and Product Development: an Infrastructure for Engagement," in *Proceedings of Participatory Design Conference (PDC'02)*, (Sweden), pp. 144–161, 2002.

[280] C. Moeckel, "From user-centred design to security: Building attacker personas for digital banking," in *Proceedings of the 10th Nordic Conference on Human-Computer Interaction (NordiCHI'18)*, Extended abstract, (Oslo, Norway), pp. 892–897, ACM, 2018.

[281] C. Moeckel, "Building attacker personas in practice — a digital banking example," in *Proceedings of the 2018 32nd British Human Computer Interaction Conference (British HCI'18)*, (Belfast, UK), ACM, July 2018.

[282] C. Moeckel, "Researching Sensitive HCI Aspects in Information Security: Experiences from Financial Services (position paper)." Available via `https://bit.ly/3frewLP`, May 2019. Sensitive Research, Practice, and Design in HCI Workshop: Conference on Human Factors in Computing Systems (CHI'19), Glasgow, United Kingdom.

[283] B. Mullings, "Insider or outsider, both or neither: some dilemmas of interviewing in a cross-cultural setting," *Geoforum*, vol. 30, pp. 337–350, 1999.

[284] D. Lønsmann, *Negotiating Positionality in Ethnographic Investigations of Workplace Settings: Student, Consultant or Confidante?*, pp. 13–36. London: Palgrave Macmillan UK, 2016.

[285] J. Henrich, S. J. Heine, and A. Norenzayan, "The weirdest people in the world?," *Behavioral and Brain Sciences*, vol. 33, no. 2-3, pp. 61–83, 2010.

[286] C. Moeckel, "Usability and Security in EU E-Banking Systems — Towards an Integrated Evaluation Framework," in *Proceedings of 2011 IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT'11)*, (Munich, Germany), pp. 230–233, ACM, July 2011.

[287] Verizon, "Data Breach Investigations Report (DBIR)." https://www.verizonenterprise.com/verizon-insights-lab/dbir, 2018. Last accessed 1st August 2020.

[288] VERIS Community, "The VERIS Community Database (VCDB) — problem statement." `http://veriscommunity.net/vcdb.html`, 2018. Last accessed 1st August 2020.

[289] J. Salminen, H. Kwak, J. Santos, S. Jung, J. An, and B. Jansen, "Persona perception scale: Developing and validating an instrument for human-like representations of data," in *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA'18)*, ACM, Apr. 2018.

[290] I. Dey, *Grounding Grounded Theory: Guidelines for Qualitative Inquiry*. Academic Press, 1999.

[291] R. F. Dam and T. Y. Siang, "Stage 2 in the Design Thinking Process: Define the Problem and Interpret the Results." `https://www.interaction-design.org/literature/article/stage-2-in-the-design-thinking-process-define-the-problem-and-interpret-the-results`, Jan. 2020. Interaction Design Foundation. Last accessed 1st August 2020.

[292] IDEO.org, "Design Kit: Bundle Ideas." `https://www.designkit.org/methods/30`. Last accessed 1st August 2020.

[293] T. Brown, "Design Thinking," *Harvard Business Review*, pp. 1–10, June 2008.

[294] L. Kimbell, "Rethinking Design Thinking: Part I," *Design and Culture*, vol. 3, no. 3, pp. 285–306, 2011.

[295] C. Plain, "Build an Affinity for K-J Method," *Quality Progress*, vol. 40, no. 3, p. 88, 2007.

[296] B. Martin and B. Hanington, *Universal Methods of Design: 100 Ways to Research Complex Problems, Develop Innovative Ideas, an Design Effective Solutions*. Rockport, 2012.

[297] K. Holtzblatt and H. Beyer, *Contextual Design — Evolved (Synthesis Lectures on Human-Centered Informatics)*. Morgan & Claypool Publishers, Oct. 2014.

[298] J. Simonsen and K. Friberg, *Situated Design Methods*, ch. Collective Analysis of Qualitative Data, pp. 99–118. The MIT Press, 2014.

[299] G. Harboe and E. M. Huang, "Real-world affinity diagramming practices: Bridging the paper-digital gap," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, (New York, NY, USA), pp. 95–104, Association for Computing Machinery, 2015.

[300] C. Maher, M. Hadfield, M. Hutchings, and A. de Eyto, "Ensuring Rigor in Qualitative Data Analysis: A Design Research Approach to Coding Combining NVivo With Traditional Material Methods," *International Journal of Qualitative Methods*, vol. 17, no. 1, 2018.

[301] S. Bødker and E. Christiansen, "Scenarios as springboard in CSCW design," in *Social Science, Technical Systems and Cooperative Work* (S. S. G. Bowker, W. Turner, and L. Gasser, eds.), pp. 217–234, Lawrence Erlbaum, 1997.

[302] J. Pruitt and J. Grudin, "Personas: Practice and Theory," *Proceedings of the 2003 Conference on Designing for User Experiences (DUX'03)*, pp. 1–15, Jan. 2003.

[303] J. Billestrup, J. Stage, L. Nielsen, and K. S. Hansen, "Persona Usage in Software Development: Advantages and Obstacles," in *7th International Conference on Advances in Computer-Human Interactions (ACHI'14)*, pp. 359–364, 2014.

[304] K. J. Knapp, T. E. Marshall, R. K. Rainer, and F. N. Ford, "Information security: management's effect on culture and policy," *Information Management & Computer Security*, vol. 14, pp. 24–36, Jan. 2006.

[305] L. Nielsen and K. S. Hansen, "Personas is applicable: a study on the use of personas in Denmark," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'14)*, pp. 1665–1674, Apr. 2014.

[306] K. Caine, "Local Standards for Sample Size at CHI," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI'16)*, pp. 981–992, ACM, 2016.

[307] TheCityUK, "Key facts about UK-based financial and related professional services." `https://www.thecityuk.com/assets/2019/Report-PDFs/b258573748/Key-facts-about-UK-based-financial-and-related-professional-services-2019.pdf`, May 2019. Last accessed 1st August 2020.

[308] J. E. Bartlett II, J. W. Kotrlik, and C. C. Higgins, "Organizational Research: Determining Appropriate Sample Size in Survey Research," *Information Technology, Learning, and Performance Journal*, vol. 19, no. 1, pp. 43–51, 2001.

[309] Qualtrics Experience Management, "Determining sample size: how to make sure you get the correct sample size." `https://www.qualtrics.com/experience-management/research/determine-sample-size`, 2020. Last accessed 1st August 2020.

[310] University of St Andrews Centre of Educational Enhancement and Development, "Statistics Support: Analysing Likert Scale/Type Data." `https://www.st-andrews.ac.uk/media/ceed/students/mathssupport/Likert.pdf`, 2020. Last accessed 1st August 2020.

[311] The Open University, "SPSS Statistics Tutorial 5: Cronbach's Alpha." `http://www.open.ac.uk/socialsciences/spsstutorial/intermediate/cronbachs-alpha`, Sept. 2018. Last accessed 1st August 2020.

[312] J. A. Gliem and R. R. Gliem, "Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales," in *Midwest Research to Practice Conference in Adult, Continuing, and Community Education*, (`https://scholarworks.iupui.edu/bitstream/handle/1805/344/Gliem&Gliem.pdf`), 2003. Last accessed 1st August 2020.

[313] H. N. Boone and D. A. Boone, "Analyzing Likert Data," *Journal of Extension*, 2012.

[314] C. Welch, P. Rebecca, H. Penttinen, and M. Tahvanainen, "Corporate elites as informants in qualitative international business research," *International Business Review*, vol. 11, pp. 611–628, Oct. 2002.

[315] R. J. Thomas, "Interviewing important people in big companies," *Journal of Contemporary Ethnography*, vol. 22, no. 80–96, 1993.

[316] J. Kirchherr and K. Charles, "Enhancing the sample diversity of snowball samples: Recommendations from a research project on anti-dam movements in Southeast Asia," *PLoS One*, vol. 13, Aug. 2018.

[317] M. Q. Patton, *Qualitative Research & Evaluation Methods*. SAGE Publications, 3rd ed., 2002.

[318] A. Blandford, D. Furniss, and S. Makri, *Qualitative HCI Research: Going Behind the Scenes*. Morgan & Claypool Publishers, 2016.

[319] L. Birt, S. Scott, D. Cavers, C. Campbell, and F. Walter, "Member checking: A tool to enhance trustworthiness or merely a nod to validation?," *Qualitative Health Research*, vol. 26, no. 13, pp. 1802–1811, 2016.

[320] Lloyds Bank Commercial Bank, "Cyber security guidance." `resources.lloydsbank.com/pdf/cyber_guidance_brochure.pdf`, 2017. Last accessed 1st August 2020.

[321] Barclays Bank UK, "Developments in cybercrime and cybersecurity." `https://labs.uk.barclays/cyber-security-awareness`, Nov. 2015. Last accessed 1st August 2020.

[322] K. Kaiser, "Protecting respondent confidentiality in qualitative research," *Qualitative Health Research*, vol. 19, pp. 1632–1641, Nov. 2009.

[323] Engineering and Physical Sciences Research Council (EPSRC) UKRI, "EPSRC policy framework on research data: expectations." `https://epsrc.ukri.org/about/standards/researchdata/expectations/`, 2011. Last accessed 1st August 2020.

[324] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[325] D. H. Mortensen, "How to Do a Thematic Analysis of User Interviews (with Ann Blandford)." https://www.interaction-design.org/literature/article/how-to-do-a-thematic-analysis-of-user-interviews, June 2020. Last accessed 1st August 2020.

[326] Y. Lincoln and E. G. Guba, *Naturalistic inquiry*. SAGE Publications, 1985.

[327] L. S. Nowell, J. M. Norris, D. E. White, and N. J. Moules, "Thematic Analysis: Striving to Meet the Trustworthiness Criteria," *International Journal of Qualitative Methods*, vol. 16, no. 1, 2017.

[328] UK National Crime Agency (NCA), "Pathways into Cyber Crime." https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file, 2017. Last accessed 1st August 2020.

[329] UK National Crime Agency (NCA) and National Cyber Security Centre (NCSC), "The cyber threat to UK business." https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime, 2018. Last accessed 1st August 2020.

[330] The Wall Street Journal, "Security expert Marc Goodman on cyber crime." https://deloitte.wsj.com/cio/2015/05/12/security-expert-marc-goodman-on-cyber-crime, May 2015. Last accessed 1st August 2020.

[331] C. D. Marcum, G. E. Higgins, and R. Tewksbury, "Doing time for cyber crime: An examination of the correlates of sentence length in the United States ," *International Journal of Cyber Criminology*, vol. 5, no. 2, pp. 824–835, 2011.

[332] HackerOne, "2020 bug bounty hacker report — Who are these bug bounty hackers?." https://www.hackerone.com/resources/reporting/the-2020-hacker-report, 2020. Last accessed 1st August 2020.

[333] Action Fraud UK, "Who reports fraud to us." https://www.actionfraud.police.uk/who-reports-fraud-to-us, 2020. Last accessed 1st August 2020.

[334] The Royal Bank of Scotland, "What to do if you think you're a victim of fraud or a scam." https://personal.rbs.co.uk/personal/fraud-and-security/report-fraud.html. Last accessed 1st August 2020.

[335] L. E. Daigle, *Victimology*. SAGE Text/Reader Series in Criminology and Criminal Justice, SAGE Publications, 2nd ed., 2017.

[336] BBC News, "Cyber-attack: US and UK blame North Korea for WannaCry." https://www.bbc.co.uk/news/world-us-canada-42407488, Dec. 2017. Last accessed 1st August 2020.

[337] T. Hunt, "I'm sorry you feel this way NatWest, but HTTPS on your landing page is important." https://www.troyhunt.com/im-sorry-you-feel-this-way-natwest-but-https-on-your-landing-page-is-important/, Dec. 2017. Last accessed 1st August 2020.

[338] M. Aiken, J. Davidson, and P. Amann, "Youth pathways into cybercrime." https://www.mdx.ac.uk/__data/assets/pdf_file/0025/245554/Pathways-White-Paper.pdf, Oct. 2016. Research report. Last accessed 1st of August 2020.

[339] Symantec, "Internet security threat report (vol. 24)." https://www.broadcom.com/support/security-center/publications/archive-threat-report, April 2019. Last accessed 1st August 2020.

[340] R. Holland, "The 'hacker' talent shortage: What organizations can learn from the recruitment efforts of their attackers." https://www.digitalshadows.com/blog-and-research/the-hacker-talent-shortage-what-organizations-can-learn-from-the-recruitment-efforts-of-their-attackers, Feb. 2016. In Digital Shadows corporate blog. Last accessed 1st August 2020.

[341] Y. Bhattacharjee, "How a remote town in Romania has become cybercrime central." https://www.wired.com/2011/01/ff-hackerville-romania, Jan. 2011. In WIRED. Last accessed 1st August 2020.

[342] Deutsche Telekom AG (DTAG), "Overview of current cyber attacks on DTAG sensors (logged by 180 sensors)." http://sicherheitstacho.eu/, 2020. Last accessed 1st August 2020.

[343] Project Honey Pot, "Project Honey Pot Statistics: Top Harvester Countries." https://www.projecthoneypot.org/harvester_top_countries.php, 2020. Last accessed 1st August 2020.

[344] Akamai, "Financial Services — Hostile Takeover Attempts," *State of the Internet / Security*, vol. 6, no. 1, 2020. Last accessed 1st August 2020.

[345] LexisNexis Risk Solutions, "ThreatMetrix EMEA Cybercrime Report." https://risk.lexisnexis.co.uk/insights-resources/research/cybercrime-report. Last accessed 1st August 2020.

[346] European Central Bank (ECB), "Letter from the Chair A. Enria of the Supervisory Board at the ECB: Contingency preparedness in the context of COVID-19." https://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2020/ssm.2020_letter_on_Contingency_preparedness_in_the_context_of_COVID-19.en.pdf, Mar. 2020. Last accessed 1st August 2020.

[347] PricewaterhouseCoopers LLP (PwC), "Global State of Information Security Survey." https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/global-state-of-information-security-survey.html, 2018. Last accessed 1st August 2020.

[348] D. Florencio and C. Herley, *Economics of Information Security and Privacy III*, ch. Sex, Lies and Cyber-Crime Surveys. Springer, 2013.

[349] Accenture & Ponemon Institute, "9th Annual Cost of Cybercrime Study." https://www.accenture.com/us-en/insights/security/cost-cybercrime-study, Mar. 2019. Last accessed 1st August 2020.

[350] Action Fraud UK, "Fraud & cybercrime cost UK nearly £11bn in past year and Reports to Action Fraud result in £1.7m investment fraudsters jailed." https://www.actionfraud.police.uk/news/fraud-cybercrime-cost-uk-nearly-11bn-in-past-year, 2016/2017. Last accessed 1st August 2020.

[351] Lloyd's & Cyence, "Counting the cost — Cyber exposure decoded (emerging risks report)." https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost, July 2017. Last accessed 1st August 2020.

[352] BBC News, "British Airways boss apologises for 'malicious' data breach." https://www.bbc.co.uk/news/uk-england-london-45440850, Sept. 2018. Last accessed 1st August 2020.

[353] F. Hannah, "Why do banks take different approaches to fraud?." https://www.independent.co.uk/money/spend-save/bank-account-fraud-reimburse-customers-pensioners-vulnerable/-responsibility-security-a8166316.html, Jan. 2018. Last accessed 1st August 2020.

[354] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, *The Economics of Information Security and Privacy*, ch. Measuring the Cost of Cybercrime, pp. 265–300. Springer, 2013.

[355] R. Anderson, C. Barton, R. Böhme, R. Clayton, C. Ganan, T. Grasso, M. Levi, T. Moore and M. Vasek, "Measuring the Changing Cost of Cybercrime," in *18th Annual Workshop on the Economics of Information Security (WEIS'19)*, 2019.

[356] R. Henry, "Bank Liability for Fraudulent Payments." https://collyerbristow.com/longer-reads/bank-liability-for-fraudulent-payments, May 2017. Collyer Bristow LLP. Last accessed 1st August 2020.

[357] J. Kavala, "Customer Liability In The Age Of Digital Banking." https://financialit.net/blog/fraud-management/customer-liability-age-digital-banking, Aug. 2017. Financial IT. Last accessed 1st August 2020.

[358] Trendmicro, "Banks Under Attack: Tactics and Techniques Used to Target Financial Organizations." https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/banks-under-attack-tactics-and-techniques-used-to-target-financial-organizations, Feb. 2018. Last accessed 1st August 2020.

[359] F-Secure, "Cyber Threat Landscape for the Finance Sector." Available via https://blog.f-secure.com/cyber-threat-landscape-for-the-finance-sector, July 2019. Last accessed 1st August 2020.

[360] Kaspersky Security Bulletin, "Cyberthreats to Financial Institutions 2020." Available via https://securelist.com/ksb-2019, 2019. Last accessed 1st August 2020.

[361] The Royal Bank of Scotland, "Responsible disclosures — Security disclosures for professionals." https://personal.rbs.co.uk/personal/security-centre/responsible-disclosure.html, 2018. Last accessed 1st August 2020.

[362] A. Cummings, T. Lewellen, D. McIntire, A. P. Moore, and R. Trzeciak, "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the US Financial Services Sector," tech. rep., Carnegie Mellon University, Software Engineering Institute, July 2012.

[363] T. J. Tracey, *Handbook of Applied Multivariate Statistics and Mathematical Modeling*, ch. Analysis of Circumplex Models, pp. 641–664. Academic Press, 2000.

[364] M. B. Gurtman and A. L. Pincus, *Handbook of Psychology, Research Methods in Psychology*, ch. The Circumplex Model: Methods and Research Applications, pp. 407–428. John Wiley & Sons, 2003.

[365] M. B. Gurtman, "Exploring Personality with the Interpersonal Circumplex," *Social and Personality Psychology Compass*, vol. 3, 2009.

[366] M. B. Gurtman, *The Encyclopedia of Clinical Psychology*, ch. Circumplex Models, pp. 507–518. John Wiley & Sons, 2014.

[367] G. S. Acton and W. Revelle, "Evaluation of Ten Psychometric Criteria for Circumplex Structure," *Methods of Psychological Research Online*, vol. 9, no. 1, 2004.

[368] M. K. Rogers, *Cybercrimes: A Multidisciplinary Analysis*, ch. The Psyche of Cybercriminals: A Psycho-Social Perspective, pp. 217–235. Springer, 2011.

[369] J. R. C. Nurse, P. A. Legg, O. Buckley, I. Agrafiotis, G. Wright, M. Whitty, D. Upton, M. Goldsmith, and S. Creese, "A Critical Reflection on the Threat from Human Insiders — Its Nature, Industry Perceptions, and Detection Approaches," in *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS'14)* (T. Tryfonas and I. Askoxylakis, eds.), vol. 8533 of *Lecture Notes in Computer Science (LNCS)*, pp. 270–281, Springer, 2014.

[370] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf, 2011. Lockheed Martin Corporation. Last accessed 1st August 2020.

[371] Deloitte, "7 Stages of Cyber Kill Chain Supplementary Reading." https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf, July 2017. Last accessed 1st August 2020.

[372] K. Goodwin, *Designing for the Digital Age: How to Create Human-Centred Products and Services*. Wiley, 2009.

[373] Getty Images — iStock database, "Source for attacker persona images — IDs for purchased images: 82011555, 247519731, 249380561, 125323949, 125705417, 117226075, 249461806." https://www.istockphoto.com, 2018. Last accessed 1st August 2020.

[374] ING Groep N.V., "ING.com security — Reporting vulnerabilities." https://www.ing.com/ING.com-Security.htm, 2018. Last accessed 1st August 2020.

[375] L. Nielsen, "From user to character: an investigation into user-descriptions in scenarios," in *Proceedings of the 4th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS'02)*, (London, UK), pp. 99–104, ACM, June 2002.

[376] J. M. Carroll, *Making Use: Scenario-Based Design of Human-Computer Interactions*. MIT Press. Cambridge, Mass., 2000.

[377] The Open University SPSS Statistics Tutorial, "Tutorial 5: Cronbach's Alpha." http://www.open.ac.uk/socialsciences/spsstutorial/intermediate/cronbachs-alpha/. Last accessed 1st August 2020.

[378] M. M. Lewis and L. Coles-Kemp, "Who Says Personas Can't Dance? The Use of Comic Strips to Design Information Security Personas," in *CHI '14 Extended Abstracts on Human Factors in Computing Systems (CHI EA'14)*, pp. 2485–2490, ACM, 2014.

[379] J. Grudin, "Why Personas Work: The Psychological Evidence," in *The Persona Lifecycle: Keeping People in Mind*, Morgan Kaufmann, 2006.

[380] J. Salminen, L. Nielsen, S.-G. Jung, J. An, H. Kwak, and B. J. Jansen, "'Is More Better?': Impact of Multiple Photos on Perception of Persona Profiles," *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI'18)*, Apr. 2018.

[381] T. UcedaVélez, "Risk Centric Application Threat Modeling Case Studies Examples in the PASTA Methodology." `https://versprite.com/videos/appsec-eu-2017-threat-modeling-with-pasta-by-tony-ucedavelez`, May 2017. At OWASP AppSecEU 2017. Last accessed 1st August 2020.

[382] Z. Pokorny, "What Is Threat Intelligence? Definition and Examples." `https://www.recordedfuture.com/threat-intelligence-definition`, Apr. 2019. Recorded Future. Last accessed 1st August 2020.

[383] Kaspersky Lab, "Lazarus under the hood." `https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf`, 2018. Last accessed 1st August 2020.

[384] MITRE Corporation, "Common Vulnerabilities and Exposures (CVE) List." `https://cve.mitre.org/`. Last accessed 1st August 2020.

[385] I. Green, "Extreme cyber scenario planning and fault tree analysis." `https://www.nist.gov/system/files/documents/2017/06/01/040813_cba_part2.pdf`, 2013. At RSA Conference 2013. Last accessed 1st August 2020.

[386] Open Risk Manual, "Third Party Fraud." `https://www.openriskmanual.org/wiki/Third_Party_Fraud`. Last accessed 1st August 2020.

[387] Open Risk Manual, "First party fraud." `https://www.openriskmanual.org/wiki/First_Party_Fraud`. Last accessed 1st August 2020.

[388] OWASP Cheat Sheet Series, "Threat Modeling Cheat Sheet." `https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html`. Also at OWASP Summit 2017. Last accessed 1st August 2020.

[389] C. Biscoe, "7 steps to a successful ISO 27001 risk assessment." `https://www.itgovernance.co.uk/blog/7-steps-to-a-successful-iso-27001-risk-assessment`, June 2020. IT Governance Blog. Last accessed 1st August 2020.

[390] Gartner, "Addressing the Cyber Kill Chain (Full Gartner Research Report)," *Gartner LookingGlass Perspectives*, 2016.

[391] CAPEC, "Common Attack Pattern Enumeration and Classification — A Community Resource for Identifying and Understanding Attacks." `https://capec.mitre.org`. Last accessed 1st August 2020.

[392] OWASP, "Application Threat Modeling." `https://www.owasp.org/index.php/Application_Threat_Modeling`. Last accessed 1st August 2020.

[393] IBM RegTech Innovations Blog, "Client Stories — Putting smart to work: Raising Cora." `https://www.ibm.com/blogs/regtech/putting-smart-work-raising-cora/`, Mar. 2018. AI Banking Client Stories. Last accessed 1st August 2020.

[394] N. Davoust, "Agile and Continuous Threat Models." `https://www.rsaconference.com/industry-topics/presentation/agile-and-continuous-threat-models`, Apr. 2018. At RSA Conference 2018, San Francisco, US. Last accessed 1st August 2020.

[395] OWASP, "Agile Software Development: Don't Forget EVIL User Stories." Available via `https://www.linuxsecrets.com/owasp-wiki/index.php/Agile_Software_Development:_Don't_Forget_EVIL_User_Stories.html`, Aug. 2011. Last accessed 1st August 2020.

[396] B. Krebs, "Malware Evolution Calls for Actor Attribution?." `https://krebsonsecurity.com/2015/05/malware-evolution-calls-for-actor-attribution`, May 2015. Krebs on Security. Last accessed 1st August 2020.

[397] C. Moeckel, "Attacker-Centric Thinking in Security — Perspectives from Financial Services Practitioners," in *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES'20)*, ACM, 2020 *(forthcoming)*.

Appendices

A

Supplementary Narrative Scenarios

A.1 Narrative scenario 1 for Bruno, the gang leader

Bruno has been part of the cybercrime world for almost a decade now. He was an outstanding student — incredibly focussed without great interest in socialising with his classmates, he started writing simple computer programmes aged 11 and excelled in mathematics, winning several competitions in St. Petersburg where he grew up. With glowing recommendation letters, Bruno started studying computer science at Lomonosov Moscow State University just after he turned 17.

He continues to write programmes on the side, both for making some extra money (he has written code for an accounting software) and for improving his skills. This is the moment where things turn — he starts spending more time in hacker forums, launching his first small intrusion attacks and learning about malicious programmes. He now only has one aim: creating something that was better than anything else that existed out there. He got so obsessed that he left two semesters before his graduation and concentrated on his programming — with success: he has produced the first version of Ares, an incredibly powerful malware package.

"*I had written something powerful: the first draft of Ares. I was 22 years old.*[57]"

After some initial testing, Bruno decides to distribute his malware as a kit to other criminals, enabling them to infect user systems with the malware, launching customised trojan attacks and to syphon off money from bank accounts all over the world. But true to his personality, he is driven to make this the best product possible for his 'customers' — Bruno works on improving the Ares code tirelessly, creating an ultra-efficient and adaptable software, offering many variants to satisfy the needs of his criminal client base.

"*It wasn't just one thing I was involved in — there was all the new variants and the network.*[58]"

Bruno is a hard worker with business sense and a clear vision for ultimate success, so he doesn't stop there and diversifies the business further. Using his own software, he also starts building a large bot net to enable large-scale attacks and to rent out some parts to other criminals as a service. Not necessarily something he had al-

[57] Based on Graff, "Inside the hunt for Russia's most notorious hacker", in WIRED, https://www.wired.com/2017/03/russian-hacker-spy-botnet, 21st March 2017. Last accessed 1st August 2020.

[58] Based on McClatchy, "Justice Department is stepping up war on cyber crooks", in The Herald/Fort Mill Times, http://www.heraldonline.com/news/local/community/fort-mill-times/article11560898.html, 2nd June 2014. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

ways planned, but true to his character, he is about to set up one of the largest botnets in the world.

But more importantly, and for the first time in his life, Bruno realises that to truly take his venture to the next level, he will need support. As the business grows bigger, he starts 'employing' a number of people to offer customer support and market the product via underground channels — he however makes very sure that these lower-skilled helpers are kept at arm's length from his business. This changes when some of the network of power users approach him about customising the code for their needs and he realises that some of their skills and connections in the underground world may add real value to his business. After a careful evaluation of their capabilities and trustworthiness (he sets them a task to think of a new attack variant for mobile banking systems), he decides to let five of these highly-skilled criminals in on some parts of the business and establishes a new 'inner circle' — his former one-man band business is starting to grow into a networked organisation. He and his deputies form a tightly knit small group at the top, each with their own area of responsibility (such as bug testing or larger customisation tasks), however Bruno always keeps control and ownership over the code and the botnet.

"*There is no limit — the guys know that if they can find a way to make more, they will be rewarded.*[59]"

Like managing people within a legal business structure, running a group of cybercriminals is not easy. But Bruno knows everyone is only in it for themselves: he manages them carefully and watches his back at all times. He is not a big fan of offering people one-time incentives like flashy cars (like some others do), although Bruno makes sure that all his best collaborators get their fair share. After all, if they can grow the business in new ways, they should know that they will be rewarded and that working hard pays off.

And it's not that Bruno does not have any ethics — it's just very different to conventionally accepted moral values: he believes in pure skill and true determination combined with hard work as well as loyalty (to the right people) rather than rules, laws and governments.

Now that Bruno has reached the 'top' and runs one of the biggest botnets in the world, he is not one to sit back and relax — he is in a continuous arms race with security researchers and the authorities trying to gain control over the large botnet infrastructure he is running. Only a little while ago he lost over half the botnet machines when a group of researchers tried to take over the network by re-routing the traffic to servers under their control — only a second layer of defence in the network the researcher overlooked and a hastily written software update that was pushed out to his network got him back in full control. This was definitely a warning — he knows that it is only a matter of time for the other side to come back stronger.

"*I really didn't think they could do this and take the network down... they got pretty close this time...*[3]"

But it's not just legal enforcement he always has to be ahead of — he knows that he is playing a dangerous game surrounded by other dangerous criminals and there could always be someone else who would want him to disappear. Of course, Bruno takes highest care of his personal security — his family is always accompanied by two of his most trusted and best guards.

The one thing that gets to him about his current life is that with his increasing success, he fears that his family (wife and five year old daughter) has become a target for investigators and other criminals. He therefore had to make the decision to hide his family at a secret location near where their family home used to be. He truly misses the days they all spent together out on the lake in the summer, but deems it crucial that his family stays hidden away to be safe — this might change one day when he gives up his business.

"*I like living a good, quiet life here with my family. I also enjoy fishing in the summer.*[60]"

[59] Based on "Cybercrime boss offers a Ferrari for hacker who dreams up the biggest scam", in The Independent, 10th May 2014, no longer available online. Included in BCS dataset [35], Appendix B.

[60] Based on FBI Cyber Most Wanted "EVGENIY MIKHAILOVICH BOGACHEV — online profile", https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-Bogachev. Last accessed 1st August 2020. Included in FBI dataset [36], Appendix B.

A.2 Narrative scenario 2 for Victor, the cyber thief

Viktor grew up with two brothers near Constanța in Romania, in the Dobruja region on the Black Sea coast. His parents ran a small private hotel for tourists visiting the nearby Danube delta (and they still do, with his younger brother taking over the business now). He had a happy and protected childhood in the small town, but became increasingly bored as an older teenager, spending a lot of time surfing the internet and as a result, his grades dropped. Rather than going to university, he took courses on web design and IT at a local college. To make money, he helped local businesses and the council with their IT. And he was waiting for something 'good' to happen to him.

At the age of 22, Viktor received a call from his older brother who had moved to the UK a few years earlier, asking him whether he wanted to join him there and set up a web design business with a friend. Excited about the change and to reunite with this brother, Viktor jumped on a plane to try his luck and make a better living.

"*Our friends asked whether I wanted some extra cash for a favour...*[61]"

After settling in Essex (near London) in a small flat with his brother and a friend, it doesn't take long for Viktor to get involved in cybercrime. A friend of his brother asks him for a favour as he has 'great programming skills' - Viktor realises quickly that this might not be entirely legal.

But making money designing websites in London is not exactly easy — the competition is immense and Viktor feels employers prefer contractors with better English language skills (after all, he's still learning). So given his difficulties to find his feet in the UK, he doesn't pull back and goes along with it — after all, his dad always had to use 'creative measures' to keep the business afloat back home. And one thing he doesn't want is needing to go back home. A financially rewarding, easy job is just too tempting for him.

"*I am no criminal mastermind or something... I am just a normal guy who wants to do stuff... almost anyone can do it...*[62]"

Before he knows it, he's been part of a small gang in Essex defrauding UK bank customers — all he did was help them to set up their computer systems and software. Most importantly, he must ensure that the group stays anonymous and can't be easily traced. Viktor is a clever guy and gets things quickly, so although the leader of the group tries to keep him 'out of the loop' and doesn't want him to understand everything about the gang's activities, he gathers that the group uses the Zeus malware kit for the fraud scheme. He receives £20,000 for the job — a large sum for him.

When the groups asks him again, Viktor isn't tempted by their offer — he already knows enough about how much money there is to be made and thinks he will be able to do better by himself. His brother and their flatmate are also up for the idea, encouraged by the money that Viktor has made — they have already started on their research.

And going in for themselves is — by chance or pure luck — the right decision, as the Essex gang Viktor worked for are all arrested and subsequently charged with fraud and money laundering. When he hears this however, it doesn't deter him at all, but motivates him to do better than them. For the first time in his life, Viktor feels empowered and incredibly driven.

"*The group only lasted for a short time, but they made a lot of money — I knew they may get caught...*[63]"

Because Viktor has made his initial experiences with the Zeus malware kit and there still seems to be quite a bit of money to be made, he doesn't see the point in changing tack now and 'purchases a license' for $1,500 via a dark web contact. But he's not one to run into this blindly — from his recent experience, he thinks that the longer they run their fraud scheme, the higher the chance they will get caught. Viktor is not prepared to risk this by poor planning — he doesn't want his parents to see him go to prison after all. He therefore spends a lot of time planning the 'first strike' and already lines people up for the 'aftercare' of the attack, e.g. to launder the money or help them disappear quickly.

[61] Based on "Hacker from Cromhall who committed credit card fraud of £26.9m is jailed", in Gazette/Gloucester Citizen, goo.gl/9Qwzmd, 14th June 2012. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

[62] Based on "Cybercrime: Latest research suggests cybercriminals are not as 'anonymous' as we think," from Oxford University News, http://www.ox.ac.uk (goo.gl/ckBkea), 8th August 2017. Last accessed 1st August 2020.

[63] Based on "Police charge 11 over Zeus cybercrime scam" in The Register, https://www.theregister.co.uk/2010/09/30/zeus_e_crime_charges, 30th September 2010. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

"*Once we got into it, there were loads of opportunities, not just banking stuff... it was too easy almost..*[64]"

In the meantime, his brother Cris and friend Emil are funding their life with a number of 'sideline gigs' — they take payments for goods and services on online marketplaces (eBay mainly) without the purchaser receiving them. While they start off with smaller items such as mobile phones or computers, they soon move to cars and other expensive items. In addition, the group also infiltrates business accounts of legitimate businesses — they get customers to pay their bills into fraudulent accounts opened by them. Viktor is not sure these are sustainable ideas (and he doesn't want to draw attention to themselves), but they have promised him that they will stop once the trojan attack pays off. Plus the money is good.

"*It was 5 weeks only... we did 3,000 accounts and got like £675,000...*[65]"

After some initial small-scale pilot runs that make a few thousand pounds for the trio, they decide for a month long attack focussing on a UK bank (they choose the one they deem to have the weakest level of online banking security). The attack is a tremendous success for the fraudsters, giving them just under half a million pounds after some outgoings (like paying people to launder or cash out the funds). While Viktor doesn't know whether the authorities are close to finding them or not, they decide to lay low for a couple of years and only take a small amount of the money — mainly to rent a larger flat, buy a car and send some money home to their families. The rest they re-invest in planning their next fraud. This is not entirely voluntary: the banks are catching up on their online banking protection and mobile banking becomes more widespread amongst UK customers — all things that make the life of fraudsters such as Viktor, who is not a brilliant programmer himself, more difficult. This doesn't put him off though — he knows there will always be ways of making money through some kind of fraud — he is already looking outside of banking.

"*It's not that we can buy a castle back home just now; we will invest in the next gig and keep making money...*[66]"

Maybe surprisingly, Viktor does spend a lot of time thinking about how he ended up where he is — after he read a newspaper piece on an elderly lady losing her life savings in a banking scam, he's not so sure about his actions only harming the banks (still, it's their fault for not securing their systems better!). Nevertheless, he regularly thinks about an exit route — he wants to run a successful, legitimate business one day. And most importantly, while he likes living with Cris and Emil, he knows that his dream is to have a family with at least 3 children and a nice house with a large garden. And he is sure this won't be in the UK either.

"*Yes, I do have the dream of one day going legit...*[67]"

[64] Based on "Going, going, done: Trio of prolific auction fraud fraudsters jailed" in The Register, https://www.theregister.co.uk/2016/09/20/auction_fraud_trio_jailed, 20th September 2016. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B (as Action Fraud Police UK).

[65] Based on "Zeus Trojan raids 3,000 UK bank account" in ComputerWorld UK, https://www.computerworlduk.com/it-vendors/zeus-trojan-raids-3000-uk-bank-accounts-3234912, 10th August 2010. No longer available online, last accessed 30th March 2018.

[66] Based on "Barclays: 'Cyber criminals aren't buying castles in eastern Europe, they are investing in the next malware'" in Yorkshire Post, https://www.yorkshirepost.co.uk/news/barclays-cyber-criminals-aren-t-buying-castles-in-eastern-europe-they-are-investing-in-the-next-malware-1-7302921, 11th June, 2015. No longer available online, last accessed 30th March 2018.

[67] Based on "What Drives Eastern European Cybercriminals?" in BankInfoSecurity, https://www.bankinfosecurity.com/interviews/what-drives-eastern-european-cybercriminals-i-3541, 10th April 2017. Last accessed 1st August 2020.

A.3 Narrative scenario 3 for Allie, the insider informant

Allie grew up in the North of England, in a small village (her mother would call it 'quaint') with three siblings. She enjoyed her childhood and teenage years at the local all-girls school, playing field hockey and netball with her friends. Just after she completed her very good A-levels and was about to go to university to study languages, her parents announced their divorce — Allie reacted badly and went to Australia for a year, working on a farm.

When she returned, she started studying Digital Media at the University of Surrey, away from her family and closer to London, where many of her friends are. She isn't angry at her parents, more sad that 'an era has come to an end'.

"*I am sure everyone who knows me would describe my character as 'impeccable'. I have been a fundraiser for numerous charities and always want the best for my parents, siblings and friends — they would never believe that I could get involved in anything illegal...*[68,69]"

After graduating (first class honours degree), she secures a place on a prestigious digital technology graduate programme for a Big 4 consulting company in London. However, feeling overlooked by her line manager when it comes to being promoted and assigned to an attractive client account, she accepts the offer of a medium-sized technology company after two and a half years.

She is much happier now — outside of work, everything is looking up, too. She has a lot of friends in London, continues to play field hockey in a regional league team and now has a boyfriend too. He works in the City and with their very decent salaries, both enjoy London and travelling abroad to the fullest. They are thinking about moving in together as well and may start looking at flats to rent soon.

Allie has been working at the technology company for a couple of years now — as a project manager on the account of a well-known high street bank. She is now being contracted to work for the bank directly as they have a shortage of staff — her manager tells her that she is best suited and she totally trusts her. She is clever and has quickly gained a promotion within the company, so this feels like a step back for her — she is disappointed. She does not feel challenged and thinks she could do so much more — privately, she is a bit angry.

"*It sounded easy enough and didn't require technical knowledge — just a few names of clients I guess...*[70]"

Six months later, her boyfriend Kieran changes jobs in the City and starts working for the investment arm of one of the competitors of the bank Allie works for. She has noticed that he now often comes home late, drinks too much and doesn't speak much with her. After some months, he asks her whether she could do him a favour and provide him with some details on the clients of the bank that she works for: 'only a couple of names, Allie, to give me a chance to get in there'.

"*It was a bit of a 'low and slow' approach — only a little bit of info once in a while...*[17]"

As Allie is currently working on the restructuring of the payments infrastructure for corporate clients for the bank, she can easily get some names for 'test cases'. For her, it doesn't seem to be that bad and there is no chance to get caught. Most of the information is available publicly somewhere anyway, she thinks. She doesn't feel too much loyalty towards the bank as she's only contracted in (although she is being treated like a long-term employee and is being trusted by colleagues). Plus she really wants to help Kieran — he means everything to her.

"*There wasn't much of a question whether I would do it for him - we were practically married...*[71]"

After providing Kieran with some client names and details about their business relationship with the bank, everything continues as nor-

[68] "Lloyds bank worker Jessica Harper jailed for £2.4m fraud." in BBC News, http://www.bbc.com/news/uk-england-london-19675834, 21st of September 2012. Last accessed 1st August 2020.

[69] "Ex Barclays manager fined after £112,000 scam claim ditched", in Herald Scotland, http://www.heraldscotland.com/news/15049474.Ex_Barclays_manager_fined_after___112_000_scam_claim_ditched, 26th January 2017. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

[70] Based on "Insider Fraud in Financial Services", Carnegie Mellon Software Engineering Institute, https://resources.sei.cmu.edu/asset_files/Brochure/2012_015_001_28207.pdf, 2012. Last accessed 1st August 2020.

[71] Based on "IT expert's £250k con uncovered after unsuspecting Sutton man receives gold bars in the post" in Sutton Guardian, http://www.suttonguardian.co.uk/news/11152224.Sutton_man_receives_gold_bars_in_the_post_after_online_scam_blunder, 16th April 2014. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

mal and he doesn't ask for any more 'favours'. The two go on a long holiday in South America and, on the last day, become engaged. Kieran gets promoted and Allie continues working for the bank. Everything seems perfect — but after a while, Kieran confides in Allie and asks her for help again. He is afraid that he will lose his job if he doesn't perform continuously. He is also struggling with debt after some of his investments haven't 'worked out' and they have been spending a lot recently. Allie is absolutely shocked, but at the same time feels proud about Kieran trusting her — she has decided she will help him.

"*I passed on details of dormant accounts holding large amounts.*[72]"

Over the next months, Allie provides Kieran with further confidential client information including identification and authentication details for the account authorisers. She also compiles a list of dormant accounts holding large amounts of money and hands it over. Although not explicitly told, Allie knows now that it is not only Kieran involved in this — there is a larger group behind this and she is fairly sure that she doesn't want to meet these people. She is also convinced now that someone else (or more than one person) in the bank is supplying information to them and she suspects fraudulent payments, fake accounts and false identity documents being used to extract the money from the bank. Kieran now collects quite a bit of money from the scam — while he uses some of it to get out of his debt, he also gives Allie quite a bit and makes sure that they have a nice life.

"*There must be some bank workers helping them. . .*[19] "

Because she knows that her contract will end in three months and she will move away from the bank, she can see an end to it and this helps her 'pull through'. Allie is careful to conceal her actions and to not act suspiciously - it's never too much information that she extracts at the same time and she watches her colleagues carefully. She has had some questions from them, but was always able to fend them off or justify herself. However, she feels that the longer she keeps going, the higher the risk will be to get caught out.

"*I think at some point the people at the bank would have caught me out.*[73]"

She often wonders how she got into this (and more importantly, did not stop). She knows what she is doing is not right, but she struggles to see who the victim is in this. And yes, she is also enjoying her good life. She also feels like she deserves it — her hard work isn't really rewarded. It's also not the case that she has been keeping all the money to herself — she has given quite a bit to her younger siblings to use for their university education.

Allie definitely doesn't see her future in cybercrime (although of course she never actually regarded herself as a cybercriminal) — she wants a quiet life with Kieran, away from all this. She hopes that she will only need to last another few months — she is sure Kieran sees it the same way. On the other hand, the extra money has provided them with certain things they couldn't have had otherwise. But she is sure she can do without it.

"*I can't really see a victim here. They won't even feel it and I am not paid enough.*[74]"

[72] Based on "Bank workers jailed for part in huge fraud that netted millions from rich Lloyds TSB customers" in Mirror UK, https://www.mirror.co.uk/news/uk-news/bank-workers-jailed-part-huge-10864216, 24th July 2017. Last accessed 1st August 2020. Originally included in BCS dataset [35], Appendix B..

[73] Based on "Ex-NatWest staffer jailed after foiled £1m hack" in Alphr.com, http://www.alphr.com/news/security/386599/ex-natwest-staffer-jailed-after-foiled-1m-hack, 17th January 2014. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

[74] Based on "Insider Fraud — Are you being defrauded from within?" in Royal Bank of Scotland (website for business customers), https://www.business.rbs.co.uk/business/security/insider-fraud.html. Last accessed 1st August 2020.

A.4 Narrative scenario 4 for Chris, the young thrill seeker

Chris has always lived near Tunbridge Wells (not too far away from London) with his parents, older sister and their two dogs. He has gone to nursery and junior school in the village where they live and then moved to secondary school in Tunbridge Wells — he's completed his A-levels there too and is now enrolled at his local college and just completed a diploma course in IT (and found both extremely boring and not exactly intellectually stimulating). Chris has a good relationship with his parents and doesn't even mind his sister too much. Chris also likes spending time with his Labrador Mojo — he has had him since his 10th birthday. Apart from that, he also has quite a few friends he has known for years in the village and also from his school (although some of them have now gone away to university). There is always something going on, especially ever since he and friends started spending more time in London.

"*I am so lucky with my family. I am sure whatever happens, they would support me...*[75]"

His friends are now used to him disappearing and not leaving his room when he is 'working on something' (sometimes for days). Chris indeed spends most of his time in front of his computer — it's never been any different, ever since he got his first computer about eight years ago. He is definitely the 'geek' of their group — and his friends sometimes joke about him being 'autistic' and his parents (mainly his mum) worry about his mental health being affected by playing too many 'online shooter games' (which he never does anyway). Everyone who knows him realises that Chris is a clever and extremely capable guy — he could have done much better at school.

"*The amount of joy and excitement I got from being able to successfully break something in which a whole team of adults tried to prevent from happening, was an amazing feeling.*[76]"

Somehow, they already feel that Chris is not one to follow the traditional path of a corporate career — he is just not interested (and he will happily tell his parents).

What his 'offline' friends, family or even his computing tutors at the college don't know, is that Chris has become a skilled hacker over the last five years. What first started off as a way of getting software like Adobe Photoshop or video editing software without paying the hefty price tag, turned into an ongoing fascination for being able to 'hack' stuff. Chris just loved the challenge - the amazement of the software working after the 'crack', but also the fact that he overcame levels of protection that a group of professionals (and more importantly, adults) had created. He was 13 then — after that, there was no turning back.

He is an eager reader and an even more eager learner — he spends endless hours on the internet, reading tutorials on things like DDoS attacks or SQL databases, but also on hacker forums reading about the newest big hacks and defacements, but also about basic skills and equipment required to become a better hacker. Chris immerses himself deeper and deeper in the hacking culture and community — as he learns more about the big names, their stories and hacks, his admiration for them and their skill grows. While he doesn't want to be a malicious 'black hat', he wants to be like them.

"*I was inspired by LulzSec. They had breached a lot of high profiles and I also wanted to become like them, but I didn't want to be a Black Hat.*[77]"

For Chris, part of this is the desire to be 'part' of the group and to be 'someone' people look up to and talk about. The more time Chris spends on forums and IRC chat rooms, the more he turns from outsider and bystander into an insider and participant.

This is also due to him getting better and better in terms of technical skills — he has defaced quite a few websites now, including schools, universities and a few council websites. And he is not keeping his successes to himself — he talks about and showcases his hacks on Twitter and on forums.

Obviously, these hacks do not impress many of the 'real' hackers — to them, he is a kid. However, one of his contacts on one the forums, a

[75] Based on "UK teenager sentenced over 'biggest' web attack" in BBC News, `http://www.bbc.com/news/technology-33480257`, 10th July 2015. Last accessed 1st August 2020. Included in Cambridge dataset [34], Appendix B.

[76] Based on Paganini, "Hacker Interview @Firox — Security Affairs", `https://securityaffairs.co/wordpress/54868/hacking/hacker-interview-firox_.html`, 30th December 2016. Last accessed 1st August 2020.

[77] Based on Paganini, "Hacker Interview — Kapustkiy", `https://securityaffairs.co/wordpress/53524/hacking/hacker-interview-kapustkiy.html`, 17th November 2016. Last accessed 1st August 2020.

hacker with the handle 'razza', is impressed by Chris' ambition and sees his potential, so he offers to become his mentor and invites him to join his 'team'.

"*Gaining membership was all about action and taking part. They really didn't have time for blowhards. And I liked that.*[78]"

There is however a catch — to become a 'full' member and gain the respect from others, Chris will need to really 'break' something. He is eager to show off his skills and his dedication — ever since he has spend more time talking to 'razza' and others in the team, Chris feels like he has learned so much. Chris decides to really go for it and targets a legacy third-party system used for mortgage applications by a UK bank. He has done a lot of work on choosing this target — the protection levels seem lower than for the rest of the bank systems.

It's not that he wants to actually gain money from this — it's more that hacking a bank seems to be one of the most difficult and dangerous tasks he can think of (and also because some of the others keep talking about targeting financial services). Using a modified hack the group has used before, Chris manages to access the database that stores the customer information of the mortgage tool — while there was never a chance that he could have transferred funds from this system, the publication of this data leak could mean severe reputational damage for the bank.

"*I knew that there were others as young as me, but they were in it for the money and nothing else...*[79]"

Chris doesn't have any criminal intention here and doesn't want to necessarily publish the data or tell the bank about it — he has proven what he can do to the group and feels like 'the king of the world' to pull off his most sophisticated and difficult hack so far. That's generally one thing that gets between him and some of the others he knows in the group. Some of the others want more — they want to make money. Or at least make their actions count for a larger campaign — for example attack payment providers for terrorists or political movements they don't support. But Chris can't really get into this — he is in it for the challenge, to have fun and for the group, he has to admit.

Chris doesn't know what the future holds really - he is still considering going to university — mainly to give him something to do and to satisfy his parents. After all, he insists he is not a real hacker, at least not a malicious one. Nevertheless, he knows that the more he got into his hacking and the more time he spends with others who are not so clear on this distinction, his moral code has somewhat blurred — he wants the hardest challenges, but is also scared to end up in court. So he doesn't know which side he will end up...

"*Sometimes I am hoping I can just finish with hacking and go to university and be normal — it's hard once you are in it and all...*[22] "

[78] Based on "Anti-Sec: Who are the world's most wanted hackers?" in BBC News, http://www.bbc.com/news/technology-17548704, 30th March 2012. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

[79] Based on "Halesowen teenager arrested as part of FBI cybercrime swoop" in Halesowen News, http://www.halesowennews.co.uk/news/11225121.Halesowen_teenager_arrested_as_part_of_FBI_cybercrime_swoop, 20th May 2014. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

A.5 Narrative scenario 5 for Az, the hacktivist

Az is originally from a medium-sized city in the Netherlands, where he grew up as the only child of his parents, who are both university professors. His teachers considered him as a rebellious student who wouldn't fit in and wasn't opposed to drugs either. With his parents often away and busy with their research work, Az spent most of his free time as a teenager within the small alternative music scene of the city, putting him into contact with many older activists, campaigning against a variety of topics, but most importantly the building of the new highway that will destroy large areas of wetlands and forest. As soon as Az had finished with high school (with an A+ in computing and IT, the only subject that ever interested him), he left the city and got on a bus to London aged 17.

Living in London is not easy in the beginning — Az is getting by on money from his parents and by sleeping on friends' couches. He nevertheless loves his new life — there are so many people to meet there who strongly care about causes like internet freedom and all other sorts of campaigning — from climate issues to animal rights. Everything changes when he meets his new girlfriend, Marina, who is a radical animal rights activist, and they move in together. He also gets a job as a junior programmer at a security company specialised in DDoS attack protection to help them pay their bills.

"*I have picked up skills, taught myself and relied on team members to teach me new skills. The team as a whole have a varied skill base from researching to DDoS and hacking. Each and everyone of us is equally important to the success of the ops....*[80]"

It is only a matter of time until Az starts helping Marina and her friends with her animal rights campaigning. His first few actions for the group are defacements of websites of whale meat sellers or their #OpWhale campaign. Az works night and day to teach himself more skills — he is not sure anymore whether he is doing it for Marina, his job or something else. After a large-scale DDoS attack that takes down the entire IT of several large fishing company, and attracts a lot of publicity, Az is contacted by another 'hacktivist' to join their 'team' for their next campaigns. At the same time, Az and Marina move to an unknown location in Europe as they fear legal repercussions from some of the larger animal rights campaigns. Az continues to work in Security remotely and enrols in an online Electrical Engineering university programme to keep his parents at bay (and paying him).

"*For me, this is about real change, not about 'lulz' or whatever you want to call it — we can change the world!* [25]"

From this point on, Az is now highly dedicated to the causes he believes in — for him, it is about unconditional justice and equality. He dreams about real political change and freedom of speech for all, but also internet freedom and anti-censorship. The new group enables him to fight for exactly that — he loves being part of a diverse group of people who believe in the same thing as him. Some of the people in the group have been supporting activists in Tunisia and Syria during the Arab Spring protests — these are the campaigns that really impress and matter to Az. But for him, not only politically motivated attacks count — it's also large corporations that he would not hesitate to work against, should they get in the way of his beliefs (he supports campaigns against copyright or fracking for example). Most importantly to him, it's all about the hack and the real impact it ultimately has rather than the glory and publicity for the group or individual hacker.

"*I think the hackers we really need to worry about are those that trusted no-one and sought no glory in the first place.*[81]"

On an every day basis, he spends a lot of time on forums (Hackforums, leakforums and nulled.io are usually first on his list), the darknet and on Twitter, reading about the latest hacks, campaigns and potential targets. He also spends a lot of time talking to others in the group, usually via IRC or through TOR browser sites. Regarding technical tools, he relies on things such as social engineering to steal accounts and password phishing, a simple DDoS tool to take down servers, an SQL injection tool and of course Kali Linux, a Linux distribution specifically designed for penetra-

[80] Based on Paganini, "Hacker Interviews — @h0t-p0ppy, the hacktivist", https://securityaffairs.co/wordpress/51038/hacktivism/hacker-interviews-h0t_p0ppy.html, 7th September 2012. Last accessed 1st August 2020.

[81] Based on "Lulzsec hackers arrested in international swoop" in BBC News, http://www.bbc.com/news/technology-17270822, 8th March 2012. Last accessed 1st August 2020. Included in Cambridge dataset [34], Appendix B.

tion testing, ethical hacking and network security assessments — it includes many security and hacking tools and Az uses it for many things such as password cracking or scanning web servers and much more.

"*On top of the technical tools, you need curiosity, willingness to learn, perseverance and a unique way of thinking.*[82,83]"

Az has just started working on his next 'op'. It's nothing out of the ordinary: the group and some of their allies are planning on launching an orchestrated, large scale distributed-denial-of-service (DDoS) attack. This time however, the target is slightly different — it's one of the world's largest payment providers rather than private or government organisation directly. The group has identified the company as a supporter of an oppressive government — directly through funding them and enabling their international payments, but also indirectly through financing arms companies that sell weapons to the country's military. The group have also listed a few other banks and financial organisations that are supporting this government and that they are looking to target as a side line to the op (these targets have also been chosen as some members claim to have insider knowledge). Az has helped to pull together the instructions for the DDoS attack for new members and outside supporters — the ideas is that the more people they can get to launch the attack, the more successful it will be. And indeed, for the hacktivists, the attack causes maximum damage: all targeted banks suffer significant service interruptions, while the payment provider cannot process international payments for almost 72 hours, disrupting individuals and businesses worldwide. The attacks are accompanied by social media campaigns and also result in huge levels of publicity from the worldwide press.

"*If you try to do this alone, the chances are higher you will get caught — because so many are doing it, the chances are next to zero...*[84]"

But despite the large success for the group, Az can't stop thinking about the fact that some members of the group have used the large attack as a distraction to launch a secondary attack to steal data and customer details. He feels that these hackers have been disguising their criminal actions under the banner of activism — while Az loves the loose and open structure of the group, this behaviour is definitely something he can't tolerate for himself. It definitely makes him think of going solo or joining another group.

"*We did actually warn them before via social media — not that that made a difference.*[85]"

While Az' ethical values differ from conventional ones and are not in line with most laws, he certainly has a moral compass — stealing money from ordinary people is not part of it. Az is certain that this won't change — he wants to continue dedicating his life to activism through his hacking for the foreseeable future. He knows the future is unpredictable, but for now, he is happy to have a girl who feels the same about activism by his side.

"*These people were not in it for our cause — it was about vandalism only... or money...*[25]"

[82] Based on Paganini, "Hacker Interviews — Revolxy from PowerfulGreekArmy", https://securityaffairs.co/wordpress/49731/hacking/hacker-interviews-revolxy.html, 26th July 2016. Last accessed 1st August 2020.

[83] Based on Paganini, "Hacker Interviews — The Riddler, the founder of the BinarySec Group", https://securityaffairs.co/wordpress/50886/hacking/hacker-interviews-binarysec.html, 3rd September 2016. Last accessed 1st August 2020.

[84] Based on "Anonymous hackers admit to charges around Mastercard and PayPal Denial of Service attack protests", in TNT, http://www.tntmagazine.com/news/uk/anonymous-hackers-admit-to-charges-around-mastercard-and-paypal-denial-of-service-attack-protests, 26th November 2012. Last accessed 1st August 2020. Included in Cambridge dataset [34], Appendix B.

[85] Based on "Bank Hacks: Iran Blame Game Intensifies" in Dark Reading, http://www.darkreading.com/attacks-and-breaches/bank-hacks-iran-blame-game-intensifies/d/d-id/1106857, 15th October 2012. Last accessed 1st August 2020. Included in BCS dataset [35], Appendix B.

A.6 Narrative scenario 6 for Kev, the money mule

Kev has not had a steady job for almost a year, despite going to the job centre and looking actively for work. He can't really find a way out of this at the moment — he can't see a route back into school or education that will lead to employment quickly. There aren't many jobs for people 'like him' in the area.

He only receives benefits and his mother keeps asking him when he will finally get a job and 'not live off her money anymore'. At the same time, she doesn't really offer him any support or ideas on where to go next. It's the same with his friends — while some of them have a job, most are in the same position and can offer little help in this matter.

It's not that he isn't enjoying his life though — Kev loves hanging out with his mates in East London, going to gigs and playing 6-a-side football. He is also really close to his family and would love to do more for them.

"*I don't really know what to do anymore — I owe so much money to my family and mates now. And then the car...*[86]"

But the lack of money and long-term opportunity is really getting him down — he is getting increasingly frustrated and desperate about his situation and can't see a future ahead. More pressing, he's got £7k debt to pay off for his car and money (£3k) to pay back he has borrowed from family and friends long ago.

When his friend Dom tells him about this mate who has been making money by doing some work online and using their bank account, he's not interested in the details, but more the money he could make that the other two are talking about.

"*My mate Dom knows this guy who got him a job and he thinks he can get me some work too...*[87]"

It seems easy enough anyway — he has got two UK bank accounts (with Santander and TSB) that are pretty much empty and that's all he needs. As agreed, Kev receives his first task via WhatsApp soon after and all he has to do is to transfer the money (it's £3,850) to another UK bank account on the day. He uses his online banking on his younger sister's laptop and it hardly takes five minutes. Over the next few days, he receives more requests like this and always completes them on time, making no mistakes. Kev can only think how easy this all was — his contact also kept his word and he got paid £500 after the first week.

He gets more jobs after this, not just transferring, but also withdrawing cash and passing it on. Even when Santander investigate and eventually close his account, he gets advice from his contact and manages to open another account with Barclays using a fake identity. The guy, Marin, seems pretty alright and Kev likes working with him.

"*The bank then sent me a very formal letter that my account was blocked and they wanted to close it — I actually got a bit scared, but nothing really happened.*[88]"

After only a few months, he is approached about doing some 'more important' work and helping with organising and recruiting others to become 'money transfer agents'. He takes over some contacts given to him, but also makes some effort to recruit via social media and through mates (although he is careful with this one — he doesn't think all of them are cut out for the job and he doesn't want to make any errors).

"*It felt good to be trusted and get more work — I now organise people myself and get more money, that's of course the best thing.*[34]"

He is making really good money now — so much that he has been able to pay back over £5k of his debt already and has been able to buy a few nice extras like new clothing and small gifts for his family (new phones for his sisters for example). He also feels much better about himself — he has got something to do, earns very good money and feels energised and motivated for the first time in a long while. He even starts a small side business with his friend Dom which sells spare parts for mobiles

[86] Based on "Cash-strapped students duped into money laundering," in The Times, https://www.thetimes.co.uk/static/connected-families/how-organised-crime-is-turning-young-people-into-money-mules, 6th August 2017. Last accessed 1st August 2020.

[87] Based on Prince, "Inside Cyber-Crime Money Mule Operations," in eWeek, http://www.eweek.com/security/inside-cyber-crime-money-mule-operations, 6th January 2011. No longer available online, last accessed 25th February 2018.Included in BCS dataset [35], Appendix B.

[88] Based on "Strange bank account transactions point to a money mule", in The Guardian, https://www.theguardian.com/money/2012/jul/07/strange-bank-account-money-mule, 7th of July 2012. Last accessed 1st August 2020.

on eBay - he gets these through an acquaintance he met through his job.

"*I deal with a lot of money now — so I asked two of my mates to help. I trust them and neither of them are stupid.*[8]"

Overall, Kev is quite happy how all this has worked out so far. There are still some things that bother him slightly about his new job and life. He knows it's not a normal job and entirely legal — after all, he has never asked where the money comes from. He wouldn't commit a crime such as stealing in a physical shop, but there just doesn't seem much of a risk in all this — his friends never got caught or if they did, the banks let them off.

Banks have never meant a lot of good to him and as he views them as the only victim in this, he doesn't feel particular guilty either. His only worry here is that his new life could stop for some reason like him being caught or jobs drying up — he just got used to it.

For now, he is trying to get the most out of this situation, pay back his debt and save some money. Kev is proud that he can help his family and he finally feels like he has a chance to build a future — he has to admit that he was quite desperate 6 months ago. He has also learned a good deal about working on the internet and managing people, which gives him a bit more confidence about running his own business or re-training.

"*Okay, I know it's not exactly right. But it's none of my business to know where the money comes from. You could call it criminal... but hey, I don't know...*[89]"

[89] Based on "Police warn public after money mule gang is jailed over £1.7 m con," , Metropolitan Police, http://news.met.police.uk, 2nd June 2017. No longer available online, last accessed 13th August 2017. Included in Cambridge dataset [34], Appendix B.

A.7 Narrative scenario 7 for Scott, the security researcher

Scott has always been interested in computers and programming, even when he was at school. He was a student leader for the computer club at his high school — but different to a lot of young students who were mainly interested in web design or app development, he has always been most interested in learning about programming languages and how to code. As he excelled in mathematics and computer science at school, it was no surprise that he started a degree in Computer Science at the University of Chicago and went on to earn an excellent Masters from there — focussing on technical courses and practical coding tutorials where possible.

"*Then in 2005, I went to my first ever DefCon in Las Vegas and my life was never the same again...*[90]"

Only relatively late Scott started getting into security, through a class on Linux vulnerabilities. Although Scott has never been someone to get overly excited about things (he's more the quiet, thoughtful type), the moment he went to the hacker convention DefCon with other students, he knew security was going to be the career pathway he wanted to follow.

Scott briefly toyed with the idea of progressing to graduate school and pursuing a PhD, but he realises that what he really wants is 'to get his hands dirty' and start working in the industry on real cases. As a top of the class graduate with several internships and recommendation letters, he secures a job as a programmer for a security firm in Silicon Valley.

"*The learning really never stops... you have to live and breathe security research!*[87]"

Over the next eight years, he works his way up to principal threat researcher at the company. It's been a steep learning curve for Scott — his extreme curiosity, good programming skills, overall passion for cyber security and a desire to constantly learn new things have helped him 'to stay on top of the game'.

For Scott, this isn't just a 9-to-5 job — over the years, he has built an impressive professional profile alongside his full-time job: a security blog with close to 100,000 visitors a month, teaching and consultancy contracts as well as the occasional media or public speaking engagement.

"*Since 2013, I have been having fun working for myself.*[91]"

In 2013, he finally decides to change things up and turns freelance as a security researcher — he is confident as he had a range of profitable offers for work coming in regularly for quite some time now (and had to turn down many jobs due to working full-time). Raising and keeping his profile up to date is more important than ever for Scott now — he spends more time on his blog, engages with others on Twitter and is even more keen to speak to the media.

"*One of my best moments was when I demonstrated a flaw I had found in mobile payment terminals at Black Hat in 2014.*[92]"

Especially in the first 18 months, it's proving difficult to get an income close to his former corporate salary. However, with regular teaching contracts, consultancy jobs and some speaking engagements at conferences and company events, he is on a good road — he now also starts getting into actual security research.

Scott is spending a lot of his time trying to find new ideas for security research — he wants to identify bugs and vulnerabilities in systems. Competitive by nature, reading about others and their findings really motivates him to look continuously for undiscovered flaws. He likes the 'pure and intellectual challenge' and the relative freedom independent research gives him over his former corporate role.

Another thing Scott enjoys about his work is that no day is ever the same. When he is not busy with a consultancy or teaching job, he will typically start his day by spending quite a bit of time reading about latest security leaks and threats on the internet (Twitter, blogs, mainstream or specialised media sites). If he has no urgent deadlines or nothing else that needs finishing urgently (like preparing teaching materials or writing security reports), he will dedicate his days to more technical research.

[90] Based on Barraco, "The Life of a Security Researcher" in AlienVault, https://www.alienvault.com/blogs/security-essentials/the-life-of-a-security-researcher, 22nd of January 2014. Last accessed 1st August 2020.

[91] Based on Cluley "About this site - professional blog", https://www.grahamcluley.com/about-this-site. Last accessed 1st August 2020.

[92] Based on Kerner "EMV Is No Silver Bullet for Payment Card Security" in eWeek, http://www.eweek.com/security/emv-is-no-silver-bullet-for-payment-card-security, 10th of August 2014. No longer available online, last accessed 30th of March 2018. Included in BCS dataset [35], Appendix B.

"*One of my most prized tools is my wide array of virtual machines containing various versions of operating systems, language packs, service packs, kernel versions, and architectures.*[37]"

Scott has a comfortable study in his family home where he does most of his work — he knows he is lucky that he can work near his family and his children every day. He uses a sophisticated set up with three large screens and a powerful laptop —one of his favourite tools is his wide array of virtual machines. He also uses many sandboxing services and other free services (e.g. VirusTotal to analyse suspicious files and URLs).

All in all, Scott likes his job as an independent security researcher, whether he works on his own or with other researchers or for companies. It suits his character and ambitions and while he enjoys the more introverted activity of researching, he also wants to publish his findings and wants people to value them and be rewarded (both financially, but also through recognition, status and a certain level of fame even). He thinks he has found something he wants to continue with for the foreseeable future.

"*That's what I got on my blog this morning from a random guy... — "We get it, you're smart, and you're good at your job - try to remember you are talking to other humans, though. Just a tip...*[93]"

There are however several frustrations for him personally. He knows that not everyone appreciates what he has to say all the time — a number of times, his often cynical comments about security on Twitter have earned him the label of being 'arrogant' or being a 'know-it-all'. But it's not only people that don't view security with the same passion as him that annoy him. Companies not reacting to him when he uses responsible disclosure processes and informs them about bugs or flaws before they become public really frustrate him. Recently, he has also felt that there have been less well-paid consultancy jobs and he suspects that some of this has been snapped up by start-ups like Synack or HackerOne revolutionising the bug bounty market. He is not overly concerned by this though — Scott is not scared of change and if it's required, he would return to a corporate role to make ends meet. After all, he has a family to look after. Very rarely, deep down inside, Scott feels down when he reads about a very sophisticated exposure of a security flaw by another researcher — thoughts about whether he is good or clever enough cross his mind. These doubts never last long — a friendly chat with a colleague or positive comments on his blog always pick him up.

"*There aren't really any boundaries. Someone can go over to the bad side or become a protector. In any event, if you're caught, you were in the wrong place at the wrong time.*[94]"

And Scott has never been tempted by the dark side of his profession. He does however know that on a handful of occasions, he has ventured into potentially illegal territory (but nothing happened). Apart from that, he is not afraid to take on and challenge companies, criminals or other researchers and make their wrongdoings public. He is however always mindful to not overstep a line that would bring his family under scrutiny. For Scott, his wife and two small children and their peaceful, middle-class life as a family near Chicago mean the most to him — not being a security researcher. Overall, Scott is happy that he can be his own boss and make a good living for them from something that he is passionate about — although it sometimes takes over his life when he works on his blog in the middle of the night or on their holiday.

[93] Based on "I'm Sorry You Feel This Way NatWest, but HTTPS on Your Landing Page Is Important" in T. Hunt, professional blog (comments section), `https://www.troyhunt.com/im-sorry-you-feel-this-way-natwest-but-https-on-your-landing-page-is-important`, 13th December 2017. Last accessed 1st August 2020.

[94] Based on "Ex-Soviet Hackers Dominate Cyber Crime World" in The Moscow Times, `https://themoscowtimes.com/news/ex-soviet-hackers-dominate-cyber-crime-world-2706`, 26th August 2013. No longer available online, last accessed 30th March 2018. Included in BCS dataset [35], Appendix B.

B

List of Sources — Grounded Theory Analysis

This appendix shows the individual source materials contained in the four datasets [34][35][36][37] as described in the data sources in Section 3.4.1 and analysed in Part II of this thesis.

BCS Cybercrime Forensics Specialist Group Briefings [35]

1. AAP, "Fraudsters paid mortgage with stolen data", in The Australian, 23rd April 2013. https://www.news.com.au/national/breaking-news/fraudsters-paid-mortgage-with-stolen-data/news-story/a4af198305af03849a472b11a141d6cb. Last accessed 1st August 2020.
2. ABC News, "FBI: Crime ring stole $70m using computer virus", in Crime-research.org, 27th October 2010. http://www.crime-research.org/news/27.10.2010/3829. Last accessed 1st August 2020.
3. N. Ammembala, "City phishing cases traced to Mumbai", in IBNLive, 1st August 2011. https://www.news18.com/news/india/city-phishing-cases-traced-to-mumbai-388333.html. Last accessed 1st August 2020.
4. Associated Press, "International cybercrime suspects to face justice in Lincoln's Federal Court", in WOWT.com, 11th April 2014. No longer available online. Last accessed 1st July 2014.
5. Azatutyun, "Computer virus 'mastermind' jailed in Armenia", 22nd May 2012. https://www.azatutyun.am/a/24589591.html. Last accessed 1st August 2020.
6. L. Baldor, "Government-backed hacker teams do most China-based data theft", in USA Today, 12th December 2011. No longer available online. Last accessed 1st July 2014.
7. B. Ballenger, "$45m stolen in hours with prepaid cards", in Money Talks News, 15th May 2013. https://www.moneytalksnews.com/45-million-stolen-in-hours-with-prepaid-cards. Last accessed 1st August 2020.
8. BBC News, "$1m-a-year botnet shut down by Microsoft and Symantec", 7th February 2013. https://www.bbc.co.uk/news/technology-21366822. Last accessed 1st August 2020.

9. BBC News, "Algerian 'bank hacker' wanted by FBI held in Thailand", 7th January 2013. https://www.bbc.co.uk/news/world-asia-20937024. Last accessed 1st August 2020.

10. BBC News, "Anonymous hackers 'cost PayPal £3.5m'", 22nd November 2012. https://www.bbc.co.uk/news/uk-20449474. Last accessed 1st August 2020.

11. BBC News, "Argentina arrests teen hacker who netted $50,000 a month", 14th Sept. 2013. https://www.bbc.co.uk/news/world-latin-america-24089050. Last accessed 1st August 2020.

12. BBC News, "Arrests over 'cyber plot' to steal from Santander bank", 13th September 2013. https://www.bbc.co.uk/news/uk-england-london-24077094. Last accessed 1st August 2020.

13. BBC News, "BlackShades: Arrests in computer malware probe", 19th May 2014. https://www.bbc.co.uk/news/uk-27471218. Last accessed 1st August 2020.

14. BBC News, "Credit card details on 20 million South Koreans stolen", 20th January 2014. https://www.bbc.co.uk/news/technology-25808189. Last accessed 1st August 2020.

15. BBC News, "Cyber gang leader Tony Colston-Hayter jailed for bank scam", 24th April 2014. https://www.bbc.co.uk/news/uk-england-london-27146037. Last accessed 1st August 2020.

16. BBC News, "Cybercriminals 'drained ATMs' in $45m world bank heist", 10th May 2013. https://www.bbc.co.uk/news/world-us-canada-22470299. Last accessed 1st August 2020.

17. BBC News, "Four arrested over London-based '£1m cyber theft'", 11th December 2013. https://www.bbc.co.uk/news/uk-england-london-25338097. Last accessed 1st August 2020.

18. BBC News, "French hacker 'admits app fraud' in Amiens", 18th October 2012. https://www.bbc.co.uk/news/world-europe-19994944. Last accessed 1st August 2020.

19. BBC News, "Mariposa botnet 'mastermind' jailed in Slovenia", 24th December 2013. https://www.bbc.co.uk/news/technology-25506016. Last accessed 1st August 2020.

20. BBC News, "More than 100 arrests, as FBI uncovers cybercrime ring", 2nd October 2010. https://www.bbc.co.uk/news/world-us-canada-11457611. Last accessed 1st August 2020.

21. BBC News, "Online bank robbers face jail time for e-crimes", 2nd July 2012. https://www.bbc.co.uk/news/technology-18672068. Last accessed 1st August 2020.

22. BBC News, "Six arrests in phishing inquiry", 9th December 2011. https://www.bbc.co.uk/news/business-16107592. Last accessed 1st August 2020.

23. BBC News, "'Sophisticated' spy camera cash machine gang jailed", 21st August 2014. https://www.bbc.co.uk/news/uk-england-london-28879973. Last accessed 1st August 2020.

24. BBC News, "SpyEye bank account hack 'mastermind' pleads guilty", 29th January 2014. https://www.bbc.co.uk/news/technology-25946255. Last accessed 1st August 2020.

25. BBC News, "US cyber-thief gets 20-year jail term", 19th May 2014. https://www.bbc.co.uk/news/technology-27472244. Last accessed 1st August 2020.

26. P. Bedard, "Cybercrime breaches $1 trillion a year, China mostly to blame", in The Washington Examiner, 21st May 2013. https://www.washingtonexaminer.com/cybercrime-breaches-1-trillion-a-year-china-mostly-to-blame. Last accessed 1st August 2020.

27. Belfast Telegraph, "10 arrested in cybercrime probe", 13th December 2012. Available on https://www.express.co.uk/news/world/364435/10-arrested-in-cyber-crime-probe. Last accessed 1st August 2020.

28. A. Bond, "Cybercriminal who stole almost £400,000 from UK students jailed", in The Mirror, 14th December 2013. https://www.mirror.co.uk/news/uk-news/manchester-cyber-criminal-olajide-onikoyi-2926762. Last accessed 1st August 2020.

29. M. Broersma, "Lone Iranian claims responsibility for SSL hack", in TechWeek Europe, 28th March 2011. Available on https://www.silicon.co.uk/workspace/lone-iranian-claims-responsibility-for-ssl-hack-24998. Last accessed 1st August 2020.

30. C. Bryan-Low, "Hackers-for-hire are easy to find", in The Wall Street Journal, 23rd January 2012. https://www.wsj.com/articles/SB10001424052970203471004577145140543496380. Last accessed 1st August 2020.

31. A. Chang, "What to do if you're worried about Russian hackers", in Top Tech News, 10th August 2014. No longer available online. Last accessed 1st July 2017.

32. Z. Chase, "How to buy a stolen credit card", in NPR, 17th June 2011. No longer available online. Last accessed 9th July 2018.

33. R. N. Charette, "This week in cybercrime", in IEEE Spectrum, 3rd Nov. 2012. No longer available online. Last accessed 9th July 2018.

34. L. Constantin, "12 suspected cybercriminals arrested in Russia along with Blackhole creator", in Network World, 6th December 2013. No longer available online. Last accessed 9th July 2018.

35. L. Constantin, "Researchers find malware targeting online stock trading software", in PC World, 18th April 2013. No longer available online. Last accessed 9th July 2018.

36. L. Constantin, "Trojan program steals log-in credentials, other sensitive data from SAP client applications", in TechWorld, 21st November 2013. Available on https://www.infoworld.com/article/2609057/trojan-program-steals-log-in-credentials-and-other-sensitive-data-from-sap-client-apps.html. Last accessed 1st August 2020.

37. Credit Today, "Police charge two in connection with cybercrime investigation", 12th December 2013. No longer available online. Last accessed 1st July 2014.

38. Crime & Justice, "Nine cybercrime gang members behind major bank fraud jailed for over 24 years", 24th April 2014. No longer available online. Last accessed 9th July 2018.

39. P. Day, "Superhackers: Inside the mind of the new cyber vandals threatening global security — by a man who used to be one", in Mail Online, 27th June 2011. http://www.dailymail.co.uk/news/article-2008841/Superhackers-Inside-minds-cyber-vandals-threatening-global-security.html. Last accessed 1st August 2020.

40. J. Decenella, "Hackers break in Citi servers, steal credit card data", in InAudit, 9th June 2011. No longer available online. Last accessed 1st July 2014.

41. J. Decenella, "Teenage hackers charged with card data theft prosecuted", in InAudit, 17th May 2011. http://inaudit.com/audit/it-audit/teenage-hackers-charged-with-card-data-theft-prosecuted-6299. Last accessed 1st August 2020.

42. H. Dixon, "Barclays hacking attack gang stole £1.3m, police say" in The Telegraph, 20th September 2013. https://www.telegraph.co.uk/news/uknews/crime/10322536/Barclays-hack-ing-attack-gang-stole-1.3-million-police-say.html. Last accessed 1st August 2020.

43. J. E. Dunn, "Gang jailed for running £11m ID theft fraud-factory", in CIO.co.uk, 11th June 2012. No longer available online. Last accessed 9th July 2018.

44. J. E. Dunn, "Metropolitan Police bust online document forging gang", in CIO.co.uk, 26th May 2011. No longer available online. Last accessed 1st July 2014.

45. J. E. Dunn, "SpyEye Trojan stole $3.2m from US victims", in Techworld, 16th September 2011. No longer available online. Last accessed 9th July 2018.

46. J. E. Dunn, "Zeus Trojan gang member gets jail for huge UK fraud", in ComputerWorld, 6th Oct. 2011. Available on https://www.csoonline.com/article/2129741/data-protection/zeus-trojan-gang-member-gets-jail-for-huge-uk-fraud.html. Last accessed 1st August 2020.

47. M. Endler, "Cybercrime 2.0: It's all about the money", in Dark Reading, 13th February 2013. https://www.darkreading.com/vulnerabilities-and-threats/cybercrime-20-its-all-about-the-money/d/d-id/110864. Last accessed 1st August 2020.

48. Evening Standard, "London schoolboy secretly arrested over 'world's biggest cyber attack'", 26th September 2013. https://www.standard.co.uk/news/crime/london-schoolboy-secretly-arrested-over-worlds-biggest-cyber-attack-8840766.html. Last accessed 1st August 2020.

49. The Express, "Cyber attack: Online criminals steal more than £400,000 from major bank", no date given. No longer available online. Last accessed 1st July 2014.

50. G. P. Felongco, "17 Chinese held in Makati City for cybercrime", in Gulf News, 27th January 2013. https://gulfnews.com/news/asia/india/17-chinese-held-in-makati-city-for-cyber-crime-1.1138286. Last accessed 1st August 2020.

51. J. Finkle, A. Viswanatha and J. Edwards, "US leads global effort to disrupt cybercrime ring", in GMA Network, 3rd June 2014. Available on https://www.businessinsurance.com/article/20140602/NEWS06/140609981. Last accessed 1st August 2020.

52. E. Flitter, "Global $200m credit card hacking ring busted", in Reuters, 5th June 2013. https://www.reuters.com/article/us-cybercrime-hacking-arrests/global-200-million-credit-card-hacking-ring-busted-idUSBRE95419G20130605. Last accessed 1st August 2020.

53. Finextra, "Trojan gang leaders jailed", 1st November 2011. https://www.finextra.com/newsarticle/23112/trojan-gang-leaders-jailed. Last accessed 1st August 2020.

54. Gloucester Citizen, "£26.9m fraud discovered in hacker's bedroom", 3rd June 2014. No longer available online. Last accessed 1st July 2014.

55. B. Goldfarb, "Halethorpe man spills secrets of international cybercrime takedown", in Arbutus Patch, 14th June 2012. https://archive.li/TZTmN. Last accessed 1st August 2020.

56. J. Goldman, "Alleged Bulgarian cybercriminal extradited to US", in eSecurity Planet, 3rd July 2013. https://www.esecurityplanet.com/network-security/alleged-bulgarian-cybercriminal-extradited-to-u.s..html. Last accessed 1st August 2020.

57. A. Gonsalves, "Cybercriminals honing Android malware skills in Russia", in Techworld, 18th May 2012. No longer available online. Last accessed 1st July 2014.

58. G. Gordon, "Justice Department is stepping up war on cyber crooks", in The State, 2nd June 2014. Available on https://www.kansas.com/news/nation-world/national/article1145091.html. Last accessed 1st August 2020.

59. I. Gowhar, "Techie held for making software for phishing", in Mid-Day, 13th September 2011. https://www.mid-day.com/articles/techie-held-for-making-software-for-phishing/134686. Last accessed 1st August 2020.

60. Gulf Times, "80 detained in global cybercrime takedown", 19th May 2014. http://www.gulf-times.com/story/392708/80-detained-in-global-cyber-crime-takedown. Last accessed 1st August 2020.

61. Halesowen News, "Halesowen teenager arrested as part of FBI cybercrime swoop", May 2014. http://www.halesowennews.co.uk/news/11225121.Halesowen_teenager_arrested_as_part_of_FBI_cybercrime_swoop. Last accessed 1st August 2020.

62. J. Hendon, "Romanian Nationals plead guilty to credit card data theft", in The Examiner, 18th September 2012. No longer available online. Last accessed 1st July 2014.

63. HostExploit, "Russian gang used customized virus bought from hacker forum on ATMs", 1st December 2010. No longer available online. Last accessed 1st July 2014.

64. HostExploit, "Suspended sentence for RBS hacker Togochakov", 14th March 2011. No longer available online. Last accessed 1st July 2014.

65. Info Security, "A look at the Russian underground cyber market", 31st October 2012. https://www.infosecurity-magazine.com/news/a-look-at-the-russian-underground-cyber-market. Last accessed 1st August 2020.

66. Info Security, "Canada: A global haven for cybercriminals", 17th June 2013. https://www.infosecurity-magazine.com/news/canada-a-global-haven-for-cybercriminals. Last accessed 1st August 2020.

67. K. Jackson Higgins, "Microsoft: Cybercrime falling into two distinct camps", in Dark Reading, 12th May 2011. https://www.darkreading.com/vulnerabilities-and-threats/microsoft-cybercrime-falling-into-two-distinct-camps/d/d-id/1097731. Last accessed 1st August 2020.

68. T. Jones, "Police arrest Romanian cybercrime syndicate", in ABC, 29th November 2012. http://www.abc.net.au/lateline/police-arrest-romanian-cyber-crime-syndicate/4400050. Last accessed 1st August 2020.

69. T. Jowitt, "Morgan Stanley was hit by Chinese hackers", in eWeek, 1st March 2011. Available on https://www.silicon.co.uk/workspace/morgan-stanley-identified-as-victim-of-chinese-hackers-22441. Last accessed 1st August 2020.

70. J. Karia, "Hacker exposes three million Iranian bank account details", in TechWeekEurope, 17th April 2012. https://www.silicon.co.uk/workspace/hacker-three-million-iranian-bank-accounts-73161. Last accessed 1st August 2020.

71. S.M. Kerner, "EMV is no silver bullet for payment card security", in eWeek, 10th August 2014. https://www.eweek.com/security/emv-is-no-silver-bullet-for-payment-card-security. Last accessed 1st August 2020.

72. J. Kirk, "UK claims cybercrime victory after phishing gang sentencing", in PC World, 11th July 2011. https://www.csoonline.com/article/2129005/malware-cybercrime/uk-claims-cybercrime-victory-after-phishing-gang-sentencing.html. Last accessed 1st August 2020.

73. T. Kitten, "$72m bank fraud scheme busted", in Bank Info Security, 27th June 2011. http://www.bankinfosecurity.com/articles.php?art_id=3790. Last accessed 1st August 2020.

74. T. Kitten, "RBS hacker's sentence too mild", in Bank Info Security, 14th February 2011. https://www.bankinfosecurity.com/rbs-hackers-sentence-too-mild-a-3348. Last accessed 1st August 2020.

75. E. Kovacs, "POS malware, RATs and banking trojans used by cybercrime group", in Softpedia, 16th April 2014. https://news.softpedia.com/news/POS-Malware-RATs-and-Banking-Trojans-Used-by-Cybercrime-Group-437880.shtml. Last accessed 1st August 2020.

76. B. Krebs, "ZeuS Trojan author in with spam kingpins", in The Sydney Morning Herald, 22nd February 2012. https://www.smh.com.au/technology/zeus-trojan-author-in-with-spam-kingpins-20120222-1tmqp.html. Last accessed 1st August 2020.

77. R. Lemos, "Thief with insider network access hijacks traffic to steal cryptocoins", in eWeek, 9th August 2014. https://www.eweek.com/security/thief-with-insider-network-access-hijacks-traffic-to-steal-cryptocoins. Last accessed 1st August 2020.

78. S. Laville, "How banks help e-crime police", in The Guardian, 24th June 2011. https://www.theguardian.com/uk/2011/jun/24/banks-help-ecrime-police-cybercrime. Last accessed 1st August 2020.

79. D. Lee, "Flame: Massive cyberattack discovered, researchers say", in BBC News, 28th May 2012. https://www.bbc.co.uk/news/technology-18238326. Last accessed 1st August 2020.

80. D. Lee, "Russian Evgeniy Bogachev sought over cybercrime botnet", in BBC News, 2nd June 2014. https://www.bbc.co.uk/news/technology-27668260. Last accessed 1st August 2020.

81. M. Lee, "Scammers known, but not arrested: ex-cop", in ZDNet, 5th March 2012. https://www.zdnet.com/article/scammers-known-but-not-arrested-ex-cop. Last accessed 1st August 2020.

82. J. Leyden, "Aussie hacker pleads guilty to banking Trojan scam", in The Register, 27th July 2010. https://www.theregister.com/Print/2010/07/27/oz_vxer_guilty_plea. Last accessed 1st August 2020.

83. J. Leyden, "Black hats attack popular Russian stock-trading software", in The Register, 18th April 2013. https://www.theregister.com/2013/04/18/online_broker_malware. Last accessed 1st August 2020.

84. J. Leyden, "Mariposa mastermind arrested in Slovenia", in The Register, 28th July 2010. https://www.theregister.com/2010/07/28/mariposa_vxer_cuffed. Last accessed 1st August 2020.

85. J. Leyden, "Russian hacker avoids jail over WorldPay heist", in The Register, 8th February 2011. https://www.theregister.com/2011/02/08/rbs_worldpay_hacker_guilty_plea. Last accessed 1st August 2020.

86. J. Leyden, "ZeuS cybercrime cookbook on sale in underground forums", in The Register, 23 March 2011. https://www.theregister.com/2011/03/23/zeus_source_code_sale. Last accessed 1st August 2020.

87. M. Liebowitz, "How cybercrime gang stole $5m in 72 hours", in NBC News, 18th January 2012. Available on http://www.nbcnews.com/id/46042544/ns/technology_and_science-security. Last accessed 1st August 2020.

88. J. Mandak and E. Tucker, "Global effort brings down cybercrime ring that stole more than $100m", Star Adviser, 2nd June 2014. http://www.staradvertiser.com/2014/06/02/breaking-news/global-effort-brings-down-cybercrime-ring-that-stole-more-than-100m. Last accessed 1st August 2020.

89. J. Menn, J. Finkle & A. Viswanatha, "US disrupts major hacking, extortion ring; Russian charged", in Reuters, 2nd June 2014. https://www.reuters.com/article/us-cybersecurity-indictment-idUSKBN0ED1GO20140602. Last accessed 1st August 2020.

90. E. Mills, "Keeping up with the hackers (chart)" in CNET, 8th February 2012. https://www.cnet.com/news/keeping-up-with-the-hackers-chart. Last accessed 1st August 2020.

91. P. Mitchell, "US alleges launderers hid $36m in Westpac accounts", in Perth Now, 29th May 2013. Available via https://www.news.com.au/finance/business/us-fraud-probe-targets-digital-currency/news-story/e95871a5ff7b35993442efaf37031292. Last accessed 1st August 2020.

92. K. Moskvitch, "Russian hacker sells home and cars to pay RBS", in BBC News, 20th September 2011. https://www.bbc.co.uk/news/technology-14989264. Last accessed 1st August 2020.

93. P. Muncaster, "Crims take to Facebook to flog ZeuS kits", in The Register, 29th April 2013. http://www.theregister.co.uk/2013/04/29/facebook_malware_zeus_toolkit. Last accessed 1st August 2020.

94. V. Narayan, "Most online criminals are educated youths: Report", in The Times of India, 20th June 2013. https://timesofindia.indiatimes.com/city/mumbai/Most-online-criminals-are-educated-youths-Report/articleshow/20672686.cms. Last accessed 1st August 2020.

95. A. Nguyen, "Police arrest online banking fraudster", in Computerworld UK, 14th March 2012. https://www.csoonline.com/article/2131144/police-arrest-online-banking-fraudster.html. Last accessed 1st August 2020.

96. Novinite, "Bulgarian Hackers Number 1 in World in ATM Skimming", 27th July 2011. https://www.novinite.com/articles/130613/Bulgarian+Hackers+Number+1+in+World+in+ATM+Skimming. Last accessed 1st August 2020.

97. J. Parusinski, "Ukraine: Hacker haven", in GlobalPost, 21st November 2012. https://www.cnbc.com/id/49926887. Last accessed 1st August 2020.

98. D. Pauli, "Fraud shop overstocked with stolen credit cards", in The Register, 29th September 2014. https://www.theregister.com/2014/09/29/fraud_shop_overstocked_with_stolen_credit_cards. Last accessed 1st August 2020.

99. P. Peachey, "Cybercrime boss offers a Ferrari for hacker who dreams up the biggest scam", in The Independent, 11th May 2014. https://www.independent.co.uk/news/uk/crime/cyber-crime-boss-offers-a-ferrari-for-hacker-who-dreams-up-the-biggest-scam-9349931.html. Last accessed 1st August 2020.

100. T. Pettifor, "Suspected 'Mr Big of UK cybercrime' questioned by police after £1.3m high-tech Barclays heist", in The Mirror, 21st September 2013. https://www.mirror.co.uk/news/uk-news/barclays-swiss-cottage-bank-heist-2289285. Last accessed 1st August 2020.

101. B. Prince, "Inside cybercrime money mule operations", in eWeek, 6th January 2011. http://www.eweek.com/security/inside-cyber-crime-money-mule-operations. Last accessed 1st August 2020.

102. M. Raftery, "Feds arrest 19 in probe of cybergroups selling stolen financial information online", in East County Magazine, March 2012. https://www.eastcountymagazine.org/feds-arrest-19-probe-cyber-groups-selling-stolen-financial-information-online. Last accessed 1st August 2020.

103. F. Y. Rashid, "Spammers require banks, suppliers, staff to run illegal trade: researchers", in eWeek, 10th June 2011. https://www.eweek.com/security/spammers-require-banks-suppliers-staff-to-run-illegal-trade-researchers. Last accessed 1st August 2020.

104. Reuters, "Ex-Soviet hackers dominate cybercrime world", in The Moscow Times, 26th August 2013. https://themoscowtimes.com/news/ex-soviet-hackers-dominate-cyber-crime-world-27060. Last accessed 1st August 2020.

105. Reuters, "Global police crackdown on 'Gameover Zeus' cybercrime botnet", in NBC News, 2nd June 2014. https://www.nbcnews.com/tech/security/global-police-crack-down-gameover-zeus-cybercrime-botnet-n120581. Last accessed 1st August 2020.

106. Reuters, "US charges Russian national for bank cybercrime", in CNBC, 2nd June 2014. https://www.cnbc.com/2014/06/02/us-charges-russian-national-for-bank-cybercrime.html. Last accessed 1st August 2020.

107. B. Rossi, "Suspected botnet master arrested in Russia", in Information Age, 25th June 2012. https://www.information-age.com/suspected-botnet-master-arrested-in-russia-2109853. Last accessed 1st August 2020.

108. M. J. Schwartz, "Bank hacks: Iran blame game intensifies", in Dark Reading, 15th October 2012. https://www.darkreading.com/attacks-and-breaches/bank-hacks-iran-blame-game-intensifies/d/d-id/1106857. Last accessed 1st August 2020.

109. M. J. Schwartz, "Russian Trojan with twist targets financial details", in Dark Reading, 23rd July 2013. https://www.darkreading.com/vulnerabilities-and-threats/russian-trojan-with-twist-targets-financial-details/d/d-id/1110875. Last accessed 1st August 2020.

110. B. Singer, "Online Trojan war ends with criminal pleas in bank account thefts", in Forbes, 26th September 2011. https://www.forbes.com/sites/billsinger/2011/09/26/online-trojan-war-ends-with-criminal-pleas-in-bank-account-thefts. Last accessed 1st August 2020.

111. A. Skelton, "Charges announced against Russian cybercrime leader", in Star Herald, 3rd June 2014. No longer available online. Last accessed 1st July 2014.

112. O. Solon, "Cybercrime becoming the easy option for traditional gangs", in The Mirror, 29th Sept. 2014. https://www.mirror.co.uk/news/technology-science/technology/cybercrime-becoming-easy-option-traditional-4344142. Last accessed 1st August 2020.

113. A. Stevenson, "Dark web black markets turning mobsters into cyber crooks", in V3, 29th September 2014. No longer available online. Last accessed 9th July 2018.

114. Strategy Page, "Information warfare: Where the bad boys are", 27th January 2013. http://www.strategypage.com/htmw/htiw/articles/20130127.aspx. Last accessed 1st August 2020.

115. The Sydney Morning Herald, "Australia's biggest ever data theft: gang busted over credit card crime", 29th November 2012. https://www.smh.com.au/technology/australias-biggest-ever-data-theft-gang-busted-over-credit-card-crime-20121129-2agzy.html. Last accessed 1st August 2020.

116. The Times of India, "4 arrested for credit card fraud", 11th June 2013. https://timesofindia.indiatimes.com/city/hyderabad/4-arrested-for-credit-card-fraud/articleshow/20530207.cms. Last accessed 1st August 2020.

117. N. Ungerleider, "How cybercriminals used banks, Facebook and Amazon for a world tour of theft", in Fast Company, 5th February 2013. https://www.fastcompany.com/3005497/how-cybercriminals-used-banks-facebook-and-amazon-world-tour-theft. Last accessed 1st August 2020.

118. University of Twente, "Russian city carries out most cyberattacks per capita: study", in Phys.org, 11th July 2011. https://phys.org/news/2011-07-russian-city-cyber-capita.htmll. Last accessed 1st August 2020.

119. C. Vallance, "Cash machines raided with infected USB sticks", in BBC News, 30th December 2013. https://www.bbc.co.uk/news/technology-25550512. Last accessed 1st August 2020.

120. Virus Bulletin, "DNS poisoning attack targeting Brazilian customers", 7th November 2011. https://www.virusbulletin.com/blog/2011/11/dns-poisoning-attack-targeting-brazilian-customers. Last accessed 1st August 2020.

121. Vision Reporter, "Police bust Internet crime gang", in New Vision, 21st July 2013. https://www.newvision.co.ug/news/1326780/police-bust-internet-crime-gang. Last accessed 1st August 2020.

122. D. Walker, "Firm highlights top site attacks on world's biggest banks", in SC magazine, 14th November 2013. https://www.scmagazine.com/firm-highlights-top-site-attacks-on-worlds-biggest-banks/article/542776. Last accessed 1st August 2020.

123. M. Ward, "Anti-Sec: Who are the world's most wanted hackers?", in BBC News, 30th March 2012. https://www.bbc.co.uk/news/technology-17548704. Last accessed 1st August 2020.

124. A. Wattanajantra, "Lucky Russian avoids prison for $10m ATM hack", in The Inquirer, 8th February 2011. No longer available online. Last accessed 9th July 2018.

125. Xinhua, "Austrian cybercrime on the increase in 2013: report", in Shanghai Daily, 12th August 2014. Available on https://www.neweurope.eu/article/austrian-cybercrime-increase-2013-report. Last accessed 1st August 2020.

126. K. Zetter, "Report: Hacktivists out-stole cybercriminals in 2011", in Wired, 22nd March 2012. https://www.wired.com/2012/03/hacktivists-beat-cybercriminals. Last accessed 1st August 2020.

127. Z. Zors, "DHS investigation uncovers cyber fraud ring members", in Help Net Security, 6th January 2011. https://www.helpnetsecurity.com/2011/01/06/dhs-investigation-uncovers-cyber-fraud-ring-members. Last accessed 1st August 2020.

Cambridge Computer Crime Database [34]

128. R. Abel, "London teen hacker sentenced in Spamhaus DDoS attacks", in SC Magazine, 13th July 2015. https://www.scmagazine.com/no-prison-time-for-spamhaus-attacker/article/532607. Last accessed 1st August 2020.

129. C. Adwent, "Suspect held in £1m-plus cyber fraud from Felixstowe company re-bailed", in East Anglian Daily Times, 25th Nov. 2015. https://www.ipswichstar.co.uk/news/suspect-held-in-1million-plus-cyber-fraud-from-felixstowe-company-re-bailed-1-4324925. Last accessed 1st August 2020.

130. H. Al-Othman, "Jail for fraudsters who conned victims out of more than £25m", in The Evening Standard, 9th January 2016. https://www.standard.co.uk/news/crime/jail-for-fraudsters-who-conned-victims-out-of-more-than-25-million-a3152511.html. Last accessed 1st August 2020.

131. A. Ballinger, "Ruislip and Kensington men jailed for roles in £4.5m fraud and money laundering operation", in Get West London, 11th July 2016. https://www.getwestlondon.co.uk/news/west-london-news/ruislip-kensington-men-jailed-roles-11598256. Last accessed 1st August 2020.

132. BBC News, "Ex-Premier League striker Nile Ranger jailed for fraud", 23rd May 2017. https://www.bbc.co.uk/news/uk-england-london-40021308. Last accessed 1st August 2020.

133. BBC News, "Hacker warned he faces jail after admitting cybercrimes", 4th December 2017. https://www.bbc.co.uk/news/uk-england-42228065. Last accessed 1st August 2020.

134. BBC News, "Lulzsec hackers arrested in international swoop", 8th March 2012. https://www.bbc.co.uk/news/technology-17270822. Last accessed 1st August 2020.

135. BBC News, "Ringleaders of £3m online 'Trojan' bank scam jailed", 1st November 2018. https://www.bbc.co.uk/news/uk-england-london-15542016. Last accessed 1st August 2020.

136. BBC News, "Online bank robbers face jail time for e-crimes", 2nd July 2012. https://www.bbc.com/news/technology-18672068.Last accessed 1st August 2020.

137. BBC News, "Three mobile: Arrests made over data breach", 18th November 2016. https://www.bbc.co.uk/news/business-38022309. Last accessed 1st August 2020.

138. BBC News, "UK hacker exploits online bank loophole to steal £100,000", 21st June 2017. https://www.bbc.co.uk/news/technology-40353758. Last accessed 1st August 2020.

139. T. Brewster, "Three phishers jailed for bank attacks", in ITPro, 12th July 2011. http://www.itpro.co.uk/634846/three-phishers-jailed-for-bank-attacks. Last accessed 1st August 2020.

140. J. Bullen, "Jailed: Unemployed fraudster who conned victims out of at least £40,000 to fund jetset lifestyle", in The Evening Standard, 24th February 2016. https://www.standard.co.uk/news/crime/jailed-unemployed-fraudster-conned-victims-out-of-at-least-40000-to-fund-jetset-lifestyle-a3188446.html. Last accessed 1st August 2020.

141. L. Cameron, "Three charged over £400,000 online fraud and money laundering", in The Scotsman, 2nd March 2017. https://www.scotsman.com/regions/aberdeen-north-east/three-charged-over-400k-online-fraud-and-money-laundering-1-4381228. Last accessed 1st August 2020.

142. M. Casserly, "Blackshades: how Police cracked down on the hackers", in Tech Advisor, 3rd July 2014. https://www.techadvisor.co.uk/feature/security/blackshades-how-police-cracked-down-on-hackers-3528675. Last accessed 1st August 2020.

143. City of London Police, "Europe-wide action targets money mule schemes", no date given. Available via https://www.europol.europa.eu/newsroom/news/europe-wide-action-targets-money-mule-schemes. Last accessed 1st August 2020.

144. City of London Police, "First of ten wanted fraudsters arrested attempting to leave the country", 22nd July 2016. No longer available online. Last accessed 1st August 2020.

145. R. Cooper, "Thomas Beeckmann jailed after being caught with hi-tech cashcard scamming kit", in Mail Online, 15th October 2011. http://www.dailymail.co.uk/news/article-2049182/Thomas-Beeckmann-jailed-caught-hi-tech-cashcard-scamming-kit.html. Last accessed 1st August 2020.

146. G. Corera, "UK teenager sentenced over 'biggest' web attack", in BBC News, 10th July 2015. https://www.bbc.co.uk/news/technology-33480257. Last accessed 1st August 2020.

147. R. Cox, "Allianz Insurance employees took £7,000 of bribes to pass on customer details", in Express & Star, 29th August 2017. https://www.expressandstar.com/news/crime/2017/08/29/allianz-insurance-employees-took-7000-of-bribes-to-pass-on-customer-details. Last accessed 1st August 2020.

148. Crime & Justice, "Eight convicted of phishing attack", 4th April 2013. No longer available online. Last accessed 1st July 2014.

149. Crime & Justice, "Four people arrested after £80,000 cash seized in following the £1m theft from UK banks", 11th December 2013. No longer available online. Last accessed 1st July 2017.

150. Crime & Justice, "Ilford phishing fraudsters jailed", 17th July 2014. No longer available online. Last accessed 1st July 2017.

151. Crime & Justice, "Phishing scammers jailed for £59m worth of fraud", 18th June 2013. No longer available online. Last accessed 1st July 2014.

152. Crime & Justice, "Two Men Arrested In Merseyside For Cyber-Crime Offences", 22nd April 2016. No longer available online. Last accessed 1st July 2017.

153. Crown Prosecution Service, "£1m fraudsters who funded notorious Nigerian organised crime gang jailed for 16 years", 2nd August 2019. https://www.cps.gov.uk/cps/news/ps1m-fraudsters-who-funded-notorious-nigerian-organised-crime-gang-jailed-16-years. Last accessed 1st August 2020.

154. Daily Mail Reporter, "Couple who took part in Nigerian gang's internet banking plot to steal £19m in 'phishing' scam are jailed", in Mail Online, 7th December 2013. http://www.dailymail.co.uk/news/article-2519854/Couple-took-Nigerian-gangs-internet-banking-plot-steal-19million-phishing-scam-jailed.html. Last accessed 1st August 2020.

155. Daily Mail Reporter, "Hacker Zachary Woodham who ruined stranger's web business 'for a game' spared jail", Mail Online, 17th May 2011. http://www.dailymail.co.uk/news/article-1387564/Hacker-Zachary-Woodham-ruined-strangers-web-business-game-spared-jail.html. Last accessed 1st August 2020.

156. P. Dinham, "Police officer and Lloyds worker husband 'laundered £113m'", in MailOnline, 25th January 2017. http://www.dailymail.co.uk/news/article-4156146/Police-officer-Lloyds-worker-husband-laundered-113m.html. Last accessed 1st August 2020.

157. M. Duell, "Teenage boffin created damaging computer software used by cyber-hackers to crash 224,000 websites around the world from the bedroom of his £170,000 family home", in Mail Online, 9th April 2016. http://www.dailymail.co.uk/news/article-3529634/Teenage-boffin-created-damaging-computer-software-used-cyber-hackers-crash-224-000-websites-world-bedroom-170-000-family-home.html. Last accessed 1st August 2020.

158. Express & Star, "Hacker who attacked Uber and Sainsbury's hands over £1m in Bitcoin", 23rd August 2019. https://www.expressandstar.com/news/uk-news/2019/08/23/hacker-who-attacked-uber-and-sainsburys-hands-over-1m-in-bitcoin. Last accessed 1st August 2020.

159. Express & Star, "Refugee jailed after frauds worth £28,000", 12th April 2016. https://www.expressandstar.com/news/crime/2016/04/12/refugee-jailed-after-frauds-worth-28k. Last accessed 1st August 2020.

160. FT Adviser, "Sentence for pregnant former Santander worker in bank fraud", 16th April 2015. https://www.ftadviser.com/2015/04/16/ifa-industry/sentence-for-pregnant-former-santander-worker-in-bank-fraud-8j2qcpGd4qqp97hzi28IGM/article.html. Last accessed 1st August 2020.

161. Get Reading, "Man convicted of cash scam", 7th June 2013. https://www.getreading.co.uk/news/local-news/man-convicted-of-cash-scam-4208756. Last accessed 1st August 2020.

162. S. Ghosh, "Ex-NatWest staffer jailed after foiled £1m hack", in Alphr, 17th January 2014. https://www.alphr.com/news/security/386599/ex-natwest-staffer-jailed-after-foiled-1m-hack. Last accessed 1st August 2020.

163. J. Grierson (and agencies), "Ringleader of gang responsible for £113m fraud jailed for 11 years", in The Guardian, 21st September 2016. https://www.theguardian.com/uk-news/2016/sep/21/feezan-hameed-fraud-gang-jailed-11-years-southwark-crown-court. Last accessed 1st August 2020.

164. Haverhill Echo, "Prison sentence for bank fraud man", 7th July 2012. No longer available online. Last accessed 1st July 2017.

165. Herald Scotland, "Ex-Barclays manager fined after £112,000 scam claim ditched", 26th January 2017. https://www.heraldscotland.com/news/15049474.ex-barclays-manager-fined-after-112000-scam-claim-ditched. Last accessed 1st August 2020.

166. T. Kirk, "Notorious teenage hacker behind 1.7m cyberattacks faces jail", in The Evening Standard, 22nd October 2016. https://www.standard.co.uk/news/crime/notorious-hacker-behind-over-17-million-cyber-attacks-faces-jail-a3376106.html. Last accessed 1st August 2020.

167. Krebs on Security, "SpamHaus, CloudFlare attacker pleads guilty", 14th Dec. 2014. https://krebsonsecurity.com/2014/12/spamhaus-cloudflare-attacker-pleads-guilty-to-computer-abuse-child-porn-charges. Last accessed 1st August 2020.

168. Krebs on Security, "ZeuS Trojan gang faces justice", 4th Oct. 2011. https://krebsonsecurity.com/2011/10/zeus-trojan-gang-faces-justice. Last accessed 1st August 2020.

169. J. Legge, "London teenager arrested over huge cyberattack", in The Independent, 26th September 2013. https://www.independent.co.uk/news/uk/crime/london-teenager-arrested-over-huge-cyberattack-8841542.html. Last accessed 1st August 2020.

170. J. Leyden, "Going, going, done: Trio of prolific auction fraud fraudsters jailed" in The Register, 20th Sept. 2016. https://www.theregister.com/2016/09/20/auction_fraud_trio_jailed. Last accessed 1st August 2020.

171. J. Leyden, "Police charge 11 over Zeus cybercrime scam", in The Register, 30th September 2010. https://www.theregister.com/2010/09/30/zeus_e_crime_charges. Last accessed 1st August 2020.

172. D. Marincu, "Man pleads guilty to hack attempt on government pensions website", in The Irish News, 1st Sept. 2017. https://www.irishnews.com/news/2017/09/02/news/guilty-plea-to-attempt-to-hack-government-pensions-website-1126057. Last accessed 1st August 2020.

173. Merton Police, "Police warn public after money mule gang is jailed over £1.7m con", 5th June 2017. https://www.facebook.com/MertonPolice/posts/police-warn-public-after-money/1719460438354306. Last accessed 1st August 2020.

174. Metropolitan Police, "Cyber-criminal gets five years for £840,000 phishing fraud", in Finextra, 21st December 2016. https://www.finextra.com/pressarticle/67507/cyber-criminal-gets-five-years-for-840k-phishing-fraud. Last accessed 1st August 2020.

175. Metropolitan Police, "Four sentenced for £500K fraud", 26th July 2019. Available via https://perma.cc/W5EP-P65U. Last accessed 1st August 2020.

176. Metropolitan Police, "Fraud gang jailed for more than 43 years", 9th May 2019. Available via https://perma.cc/W5EP-P65U. Last accessed 1st August 2020.

177. Metropolitan Police, "Gang behind high-value frauds convicted", 28th May 2019. Available via https://perma.cc/C5EN-5876. Last accessed 1st August 2020.

178. Metropolitan Police, "Group guilty of hacking email account for £3m fraud", 23rd May 2019. Available via https://perma.cc/H8YY-L4UN. Last accessed 1st August 2020.

179. Metropolitan Police, "Internet shopping fraud gang jailed", 19th November 2016. Available via http://starconnectmedia.com/600000-internet-shopping-fraud-gang-jailed. Last accessed 1st August 2020.

180. Metropolitan Police, "Met FALCON detectives smash £113m international fraud and money laundering ring", 21st September 2016. No longer available online. Last accessed 13th July 2018.

181. Metropolitan Police, "Two charged with laundering proceeds of malware crime", in Public Now, 19th March 2017. No longer available online. Last accessed 13th July 2018.

182. Metropolitan Police, "Two convicted of unlawful access to Met intel systems", 13th December 2016. No longer available online. Last accessed 1st July 2017.

183. Metropolitan Police, "Two more jailed in relation to £3m bank fraud", 8th February 2012. Available via https://www.finextra.com/pressarticle/43029/two-more-jailed-in-relation-to-3-million-bank-fraud. Last accessed 1st August 2020.

184. M. Metzger, "ATM malware gang member arrested in Romania", in SC Magazine UK, 5th October 2016. https://www.scmagazineuk.com/atm-malware-gang-member-arrested-romania/article/1476894. Last accessed 1st August 2020.

185. M. Murphy-Pyle, "IT expert's £250,000 con uncovered after unsuspecting Sutton man receives gold bars in the post", in Sutton Guardian, 16th April 2014. https://www.yourlocalguardian.co.uk/news/11152224.it-experts-250k-con-uncovered-after-unsuspecting-sutton-man-receives-gold-bars-in-the-post. Last accessed 1st August 2020.

186. S. Murray, "UK student pleads guilty after earning £315,000 from DDoS tool", in PCR, 2nd November 2016. https://www.pcr-online.biz/2016/11/02/uk-student-pleads-guilty-after-earning-315000-from-ddos-tool. Last accessed 1st August 2020.

187. R. Myers, "Bank workers jailed for part in huge fraud that netted millions from rich Lloyds TSB customers", in The Mirror, 24th July 2017. https://www.mirror.co.uk/news/uk-news/bank-workers-jailed-part-huge-10864216. Last accessed 1st August 2020.

188. NCA, "57 arrested in nationwide cybercrime strike week", 6th March 2015. No longer available online. Last accessed 13th July 2018.

189. NCA, "Accountant and two bankers jailed for stealing £390k from customers", undated. https://www.nationalcrimeagency.gov.uk/news/accountant-and-two-bankers-jailed-for-stealing-390k-from-customers. Last accessed 1st August 2020.

190. NCA, "Back to prison for cyber fraudster who dodged computer restrictions", 15th November 2016. Available via https://www.wired-gov.net/wg/news.nsf/articles/Back+to+prison+for+cyber+fraudster+who+dodged+computer+restrictions+16112016131500. Last accessed 1st August 2020.

191. NCA, "Champagne fraudster loses his fizz", 3rd July 2014. Available on https://thelondonpost.net/champagne-fraudster-jailed-for-8-years. Last accessed 1st August 2020.

192. NCA, "Cyber criminal made thousands of pounds with product-testing site for hackers", 15th January 2018. Available via https://www.wired-gov.net/wg/news.nsf/articles/Cyber+criminal+made+thousands+of+pounds+with+producttesting+site+for+hackers+16012018121500. Last accessed 1st August 2020.

193. NCA, "High rolling fraudster conned thousands out of vulnerable victims", 3rd September 2015. Available via https://www.wired-gov.net/wg/news.nsf/articles/High+rolling+fraudster+conned+thousands+out+of+vulnerable+victims+04092015151500. Last accessed 1st August 2020.

194. NCA, "Hundreds of bank accounts used to launder profits of cyber theft", 5th October 2016. Available via https://www.wired-gov.net/wg/news.nsf/articles/Hundreds+of+bank+accounts+used+to+launder+profits+of+cyber+theft+06102016111500?open. Last accessed 1st August 2020.

195. NCA, "International operation shuts down online hacking forum", 15th July 2015. Available via https://www.cybersecurity-review.com/international-operation-shuts-down-online-hacking-forum. Last accessed 1st August 2020.

196. NCA, "Multiple UK arrests in international operation to combat computer hijackers", 21st November 2014. Available via https://www.wired-gov.net/wg/news.nsf/articles/Multiple+UK+arrests+in+international+operation+to+combat+computer+hijackers+23112014080520?open. Last accessed 1st August 2020.

197. NCA, "NCA targets international cybercrime network", 3rd November 2016. No longer available online. Last accessed 13th July 2018.

198. NCA, "Operation Vulcanalia targets users of netspoof website attack tool", 12th December 2016. Available via https://www.wired-gov.net/wg/news.nsf/articles/Operation+Vulcanalia+targets+users+of+netspoof+website+attack+tool+13122016101500?open. Last accessed 1st August 2020.

199. NCA, "Operation Vivarium targets users of Lizard Squad's website attack tool", 28th August 2015. Available via https://www.wired-gov.net/wg/news.nsf/articles/Operation+Vivarium+targets+users+of+Lizard+Squads+website+attack+tool+28082015152000?open. Last accessed 1st August 2020.

200. NCA, "Organised crime group altered business emails to rip-off more than £1m", 17th May 2018. Available via https://www.wired-gov.net/wg/news.nsf/articles/Organised+crime+group+altered+business+emails+to+ripoff+more+than+1m+19052018091000?open. Last accessed 1st August 2020.

201. NCA, "Prison for prolific cyber fraudster", 17th July 2014. Available via https://www.wired-gov.net/wg/news.nsf/articles/Prison+for+prolific+cyber+fraudster+17072014121500. Last accessed 1st August 2020.

202. NCA, "Suspected DDoS attacker is charged", no date given. Available via https://www.dos-protection.co.uk/2014/06/28/. Last accessed 1st August 2020.

203. C. Neeson, "Armagh man handed nine weeks in prison for stealing £700 from grandfather", 9th April 2019. https://www.armaghi.com/news/armagh-news/armagh-man-handed-nine-weeks-in-prison-for-stealing-700-from-grandfather/85460. Last accessed 1st August 2020.

204. Nottinghamshire Police, "Two police officers and a staff member to face criminal charges", 17th November 2016. No longer available online. Last accessed 1st July 2017.

205. Nottinghamshire Police, "Former accountant jailed after admitting fraud", 22nd June 2019. Available via https://perma.cc/TE9P-GWC9. Last accessed 1st August 2020.

206. Press Association, "Gang jailed for stealing bank card details worth £16m", in The Guardian, 21st August 2014. No longer available online. Last accessed 1st July 2017.

207. M. Sauvebois, "Hacker from Cromhall who committed credit card fraud of £26.9m is jailed" in The Gloucestershire Gazette, 14th June 2012. https://www.gazetteseries.co.uk/news/9755478.hacker-from-cromhall-who-committed-credit-card-fraud-of-269m-is-jailed. Last accessed 1st August 2020.

208. Shropshire Star, "Telford Black Dragon hacker Matthew Beddoes jailed over £7m plot", 19th March 2013. https://www.shropshirestar.com/news/crime/2013/03/19/telford-black-dragon-hacker-matthew-beddoes-jailed-over-7m-plot. Last accessed 1st August 2020.

209. Shropshire Star, "Telford mother spared jail in £53m bank scam", 14th August 2013. https://www.shropshirestar.com/news/2013/08/14/telford-mother-spared-jail-in-53m-bank-scam. Last accessed 1st August 2020.

210. Square Mile News, "Insurance worker's £39,000 computer fraud on employer", 18th August 2013. http://squaremilenews.blogspot.com/2013/08/insurance-workers-39k-computer-fraud-on.html. Last accessed 1st August 2020.

211. A. Stevenson, "Digital fraudster 'tetereff' gets five years hard time", in V3, 16th July 2014. No longer available online. Last accessed 17th July 2018.

212. Sunderland Echo, "Former Newcastle United striker Nile Ranger admits online banking fraud", in The Sunderland Echo, 11th January 2017. https://www.sunderlandecho.com/news/former-newcastle-united-striker-nile-ranger-admits-online-banking-fraud-1-8328945. Last accessed 1st August 2020.

213. Surrey Police, "Six convicted for £100,000 fraud that began with a single button press", 21st February 2018. No longer available online. Last accessed 13th July 2018.

214. Swindon Advertiser, "Alan Biggins, who admitted advance fee fraud", 7th February 2013. https://www.swindonadvertiser.co.uk/news/10211000.alan-biggins-who-admitted-advance-fee-fraud. Last accessed 1st August 2020.

215. J. Taylor, "Lloyds Bank staff aided multi-million fraud", in The Metro, 18th July 2017. https://www.metro.news/lloyds-bank-staff-aided-multi-million-fraud/677788. Last accessed 1st August 2020.

216. B. Thain, "Man charged as part of police internet scam investigation", in Enfield Independent, 12th April 2013. https://www.enfieldindependent.co.uk/news/10353234.man-charged-as-part-of-police-internet-scam-investigation. Last accessed 1st August 2020.

217. E. Thomas, "Fraud trio jailed for credit card thefts", in Basildon, Canvey, Southend Echo, 11th September 2013. https://www.echo-news.co.uk/news/10664681.fraud-trio-jailed-for-credit-card-thefts. Last accessed 1st August 2020.

218. TNT magazine, "Anonymous hackers admit to charges around Mastercard and PayPal Denial of Service attack protests", 26th Nov. 2012. http://www.tntmagazine.com/news/uk/anonymous-hackers-admit-to-charges-around-mastercard-and-paypal-denial-of-service-attack-protests. Last accessed 1st August 2020.

219. West Midlands Police, "West Mids teens arrested in £1m card scam probe", 16th November 2016. No longer available online. Last accessed 1st July 2017.

220. A. Williams, "Romanian Teofil Bortos who gave ATMs a computer virus to steal £1.3m faces jail", in Mail Online, 16th December 2015. http://www.dailymail.co.uk/news/article-3362672/Romanian-gangster-helped-steal-1-3m-just-five-days-infecting-high-street-ATMs-computer-virus-faces-years-bars.html. Last accessed 1st August 2020.

221. J. Williams, "Manchester 'phishing' fraudster jailed for £1.5m student loan scam", in Manchester Evening News, 15th December 2013. https://www.manchestereveningnews.co.uk/news/greater-manchester-news/manchester-phishing-fraudster-jailed-15m-6407528. Last accessed 1st August 2020.

222. J. Williams, "Bank worker passed on customer profiles", in Manchester Evening News, 19th April 2010. https://www.manchestereveningnews.co.uk/news/local-news/bank-worker-passed-on-customer-profiles-968851. Last accessed 1st August 2020.

223. D. Worth, "Police arrest three over £1.6m ATM malware thefts", in V3, 27th October 2014. No longer available online. Last accessed 17th July 2018.

Federal Bureau of Investigation [36]

224. FBI, "Abuzar Gohari Moqadam". https://www.fbi.gov/wanted/cyber/abuzar-gohari-moqadam. Last accessed 1st August 2020.

225. FBI, "Abdollah Karima". https://www.fbi.gov/wanted/cyber/abdollah-karima. Last accessed 1st August 2020.

226. FBI, "Ahmad Fathi". https://www.fbi.gov/wanted/cyber/ahmad-fathi. Last accessed 1st August 2020.

227. FBI, "Alexsey Belan". https://www.fbi.gov/wanted/cyber/alexsey-belan. Last accessed 1st August 2020.

228. FBI, "Alexandr Sergeyevich Bobnev". No longer available online. Last accessed 1st July 2015.

229. FBI, "Amin Shokohi". https://www.fbi.gov/wanted/cyber/amin-shokohi. Last accessed 1st August 2020.

230. FBI, "Arash Amiri Abedian". https://www.fbi.gov/wanted/cyber/arash-amiri-abedian. Last accessed 1st August 2020.

231. FBI, "Behzad Mesri". No longer available online. Last accessed 26th July 2018.

232. FBI, "Bjorn Daniel Sundin". https://www.fbi.gov/wanted/cyber/bjorn-daniel-sundin. Last accessed 1st August 2020.

233. FBI, "Danial Jeloudar". https://www.fbi.gov/wanted/cyber/danial-jeloudar. Last accessed 1st August 2020.

234. FBI, "Dmitry Aleksandrovich Dokuchaev". No longer available online. Last accessed 26th July 2018.

235. FBI, "Ehsan Mohammad". https://www.fbi.gov/wanted/cyber/ehsan-mohammadi. Last accessed 1st August 2020.

236. FBI, "Evgeniy Mikhailovich Bogachev". https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev. Last accessed 1st August 2020.

237. FBI, "Firas Dardar". https://www.fbi.gov/wanted/cyber/firas-dardar. Last accessed 1st August 2020.

238. FBI, "Gholamreza Rafatnejad". https://www.fbi.gov/wanted/cyber/gholamreza-rafatnejad. Last accessed 1st August 2020.

239. FBI, "Hamid Firoozi". https://www.fbi.gov/wanted/cyber/hamid-firoozi. Last accessed 1st August 2020.

240. FBI, "Huang Zhenyu". https://www.fbi.gov/wanted/cyber/huang-zhenyu. Last accessed 1st August 2020.

241. FBI, "Igor Anatolyevich Sushchin". https://www.fbi.gov/wanted/cyber/igor-anatolyevich-sushchin. Last accessed 1st August 2020.

242. FBI, "Iranian Mabna hackers". https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers. Last accessed 1st August 2020.

243. FBI, "Iranian DDoS attacks". https://www.fbi.gov/wanted/cyber/iranian-ddos-attacks. Last accessed 1st August 2020.

244. FBI, "Jabberzeus subjects". https://www.fbi.gov/wanted/cyber/jabberzeus-subjects. Last accessed 1st August 2020.

245. FBI, "Joshua Samuel Aaron". No longer available online. Last accessed 1st July 2015.

246. FBI, "Mohammad Sadegh Ahmadzadegan". https://www.fbi.gov/wanted/cyber/mohammad-sadegh-ahmadzadegan. Last accessed 1st August 2020.

247. FBI, "Mohammad Reza Rezakhah". https://www.fbi.gov/wanted/cyber/mohammad-reza-rezakhah. Last accessed 1st August 2020.

248. FBI, "Mostafa Sadeghi". https://www.fbi.gov/wanted/cyber/mostafa-sadeghi. Last accessed 1st August 2020.

249. FBI, "Nader Saedi". https://www.fbi.gov/wanted/cyber/nader-saedi. Last accessed 1st August 2020.

250. FBI, "Nicolae Popescu". https://www.fbi.gov/wanted/cyber/nicolae-popescu. Last accessed 1st August 2020.

251. FBI, "Omid Ghaffarinia". https://www.fbi.gov/wanted/cyber/omid-ghaffarinia. Last accessed 1st August 2020.

252. FBI, "Park Jin Hyok". https://www.fbi.gov/wanted/cyber/park-jin-hyok. Last accessed 1st August 2020.

253. FBI, "Roozbeh Sabahi". https://www.fbi.gov/wanted/cyber/roozbeh-sabahi. Last accessed 1st August 2020.

254. FBI, "Sajjad Tahmasebi". https://www.fbi.gov/wanted/cyber/sajjad-tahmasebi. Last accessed 1st August 2020.

255. FBI, "Seyed Ali Mirkarimi". https://www.fbi.gov/wanted/cyber/seyed-ali-mirkarimi. Last accessed 1st August 2020.

256. FBI, "Shaileshkumar P. Jain". https://www.fbi.gov/wanted/cyber/shaileshkumar-p.-jain. Last accessed 1st August 2020.

257. FBI, "Sina Keissar". https://www.fbi.gov/wanted/cyber/sina-keissar. Last accessed 1st August 2020.

VERIS Community Database [37]

258. G. Anand, "Global connection to capital's ATM thefts", 10th August 2016. https://www.thehindu.com/todays-paper/tp-national/tp-kerala/Global-connection-to-capital-ATM-thefts/article14561531.ece. Last accessed 1st August 2020.

259. Bank Info Security, "DDoS Attacks strike three banks", 20th August 2013. http://www.bankinfosecurity.com/ddos-attacks-strike-three-banks-a-6006. Last accessed 1st August 2020.

260. Bank Info Security, "DDoS: New attacks against banks", 29th January 2014. http://www.bankinfosecurity.com/ddos-new-attacks-against-banks-a-6449. Last accessed 1st August 2020.

261. A. Barbaschow, "Hackers hit central banks in Indonesia and South Korea", 22nd June 2016. https://www.zdnet.com/article/hackers-hit-central-banks-in-indonesia-and-south-korea. Last accessed 1st August 2020.

262. BBC News, "Arrests over 'cyber plot' to steal from Santander bank", 13rd September 2013. https://www.bbc.co.uk/news/uk-england-london-24077094. Last accessed 1st August 2020.

263. BBC News, "Bank of Scotland's fax blunder leads to fine", 5th August 2013. https://www.bbc.co.uk/news/business-23572574. Last accessed 1st August 2020.

264. J. Blumenthal, "Local bank employee charged in identity theft scheme", 9th May 2016. https://www.bizjournals.com/philadelphia/morning_roundup/2016/05/td-bank-tuffour-charge-identify-theft-fraud.html. Last accessed 1st August 2020.

265. CBC News, "GM Financial customer details 'inappropriately accessed' by ex-employee", 1st August 2015. https://www.cbc.ca/news/canada/gm-financial-customer-details-inappropriately-accessed-by-ex-employee-1.3177092. Last accessed 1st August 2020.

266. C. Cimpanu, "North Korean hackers used Hermes ransomware to hide recent bank heist", 17th October 2017. https://www.bleepingcomputer.com/news/security/north-korean-hackers-used-hermes-ransomware-to-hide-recent-bank-heist. Last accessed 1st August 2020.

267. C. Cimpanu, "Retiring sysadmin fakes cyber-attack to get away with data theft", 6th September 2016. https://news.softpedia.com/news/retiring-sysadmin-fakes-cyber-attack-to-get-away-with-data-theft-507992.shtml. Last accessed 1st August 2020.

268. Cision PR, "University Bank of Ann Arbor liable for 'willful and malicious' trade secret misappropriation" 21st June 2016. https://www.prnewswire.com/news-releases/university-bank-of-ann-arbor-liable-for-willful-and-malicious-trade-secret-misappropriation-300288118.html. Last accessed 1st August 2020.

269. CNN Money, "Breach affects 40M+ credit cards", 27th July 2005. https://money.cnn.com/2005/06/17/news/master_card/index.htm. Last accessed 1st August 2020.

270. CNN Money, "Hacker hits up to 8M credit cards", 23 February 2003. https://money.cnn.com/2003/02/18/technology/creditcards/. Last accessed 1st August 2020.

271. Coconuts Bali, "Bali ATM skimming: 2 Bulgarians caught red-handed in Lovina", 19th September 2017. https://coconuts.co/bali/news/2-bulgarians-arrested-bali-using-skimmer-atm-lovina. Last accessed 1st August 2020.

272. CS Infotech, "Pakistani financial institution Allied Bank Limited hacked", 18th July 2013. https://csinfotechblog.wordpress.com/2013/07/18/pakistani-financial-institution-allied-bank-limited-hacked. Last accessed 1st August 2020.

273. Daily Mail Reporter, "Animal activists claim to have hacked into insurance company to steal financial data on badger cull supporters", 11th June 2013. https://www.dailymail.co.uk/news/article-2339351/Animal-activists-claim-hacked-NFU-insurance-company-steal-financial-data-badger-cull-supporters.html. Last accessed 1st August 2020.

274. DataBreaches, "Former employee of global financial services company charged with unauthorized access of supervisor's email account on approximately 100 occasions", 12th December 2015. https://www.databreaches.net/former-employee-of-global-financial-services-company-charged-with-unauthorized-access-of-supervisors-email-account-on-approximately-100-occasions. Last accessed 1st August 2020.

275. DataBreaches, "Now it's three: Ecuador bank hacked via Swift", 21st May 2016. https://www.databreaches.net/now-its-three-ecuador-bank-hacked-via-swift. Last accessed 1st August 2020.

276. DataBreaches, "Turkish attackers shut down Russian Central Bank website", 25th November 2015. https://www.databreaches.net/turkish-attackers-shut-down-russian-central-bank-website. Last accessed 1st August 2020.

277. F. Donnelly, "2 sentenced in Staten Island ATM-skimming case", 2nd July 2013. https://www.silive.com/news/2013/07/sentenced_in_staten_island_atm.html. Last accessed 1st August 2020.

278. J. Dwyer, "Former Washington University investment manager indicted on computer fraud charges", 2nd May 2014. https://www.bizjournals.com/stlouis/news/2014/05/02/former-washington-university-investment-manager.html. Last accessed 1st August 2020.

279. S. Edwards, "Qatar bank breach lifts the veil on targeted attack strategies", 27th April 2016. http://blog.trendmicro.co.uk/qatar-bank-breach-lifts-the-veil-on-targeted-attack-strategies. Last accessed 1st August 2020.

280. E-Hacking News, "Central Bank Of India hacked by Pakistan Cyber Army and Team MaDLeeTs", 26th November 2013. https://www.ehackingnews.com/2013/11/central-bank-of-india-hacked-by.html. Last accessed 1st August 2020.

281. E-Hacking News, "NatWest online banking service hit by DDOS attack", 28th December 2013. https://www.ehackingnews.com/2013/12/natwest-ddos-cyber-attack.html. Last accessed 1st August 2020.

282. E-Hacking News, "State Bank of Patiala hacked and defaced by Pakistani hacker", 2nd December 2013. https://www.ehackingnews.com/2013/12/state-bank-patiala-hacked.html. Last accessed 1st August 2020.

283. Ethiopian Times, "Commercial Bank of Ethiopia website hacked & data leaked by SEPO", 26th Juanary 2012. https://ethiopiantimes.wordpress.com/2012/01/26/commercial-bank-of-ethiopia-website-hacked-data-leaked-by-sepo/. Last accessed 1st August 2020.

284. I. Finkel, "HSBC loses 2.7 million customers data in turkey-attack", 13th November 2014. https://www.bloomberg.com/news/articles/2014-11-13/hsbc-loses-2-7-million-customers-data-in-turkey-attack. Last accessed 1st August 2020.

285. S. Glenn, "Fircrest teller charged with stealing $42,000 from ailing customer messed up so bad", 5th August 2015. https://www.thenewstribune.com/news/local/crime/article94019792.html. Last accessed 1st August 2020.

286. HackRead, "MasterCard website hacked by Indonesian hackers", 29th April 2015. https://www.hackread.com/indonesian-hackers-hack-mastercard-website. Last accessed 1st August 2020.

287. HackRead, "#OpGabon: Anonymous hacks, defaces Axa Insurance Group website against its support for Ali Bongo", 25th August 2013. https://www.hackread.com/opgabon-anonymous-hacks-axa-insurance-group. Last accessed 1st August 2020.

288. O. Hirt, "German IT specialist sentenced to three years for Swiss data theft", 22nd August 2013. https://www.reuters.com/article/us-swiss-datatheft/german-it-specialist-sentenced-to-three-years-for-swiss-data-theft-idUSBRE97L0I820130822. Last accessed 1st August 2020.

289. B. Honan, "European Central Bank hacked", 31st July 2015. No longer available online. Last accessed 5th December 2019.

290. E.A. Hughes, "Ex-LV employee in court over data leak ", 21st September 2016. https://www.ftadviser.com/protection/2016/09/21/ex-lv-employee-in-court-over-data-leak. Last accessed 1st August 2020.

291. P. Hurtado and C. Smythe, "Ex-JPMorgan Employee charged with stealing customer data", 28th April 2015. https://www.bloomberg.com/news/articles/2015-04-28/ex-jpmorgan-worker-arrested-by-fbi-over-theft-of-consumer-data. Last accessed 1st August 2020.

292. Infosecurity, "Second RBS outage in a week paves the way for phishing extravaganza", 9th December 2013. https://www.infosecurity-magazine.com/news/second-rbs-outage-in-a-week-paves-the-way-for. Last accessed 1st August 2020.

293. Irish Mirror, "Bank card skimming devices left on ATMs in Donegal Town for up to six months before being discovered", 14th October 2013. https://www.irishmirror.ie/news/irish-news/crime/bank-card-skimming-devices-left-2369654. Last accessed 1st August 2020.

294. The Japan Times, "Bank of Saga client data allegedly stolen, handed to suspected criminals", 19th June 2017. https://www.japantimes.co.jp/news/2017/06/19/national/crime-legal/bank-saga-client-data-allegedly-stolen-handed-suspected-criminals. Last accessed 1st August 2020.

295. D. Jorgenson, "2 men charged in connection with card-skimming devices in St. Augustine Beach", 2nd November 2013. https://www.news4jax.com/news/2017/11/02/2-men-charged-in-connection-with-card-skimming-devices-in-st-augustine-beach. Last accessed 1st August 2020.

296. The Korea Times, "EconomyCustomer data at SC, Citibank leaked", 11th December 2013. http://www.koreatimes.co.kr/www/news/biz/2013/12/488_147800.html. Last accessed 1st August 2020.

297. E. Kovacs, "Gaza Hackers Deface Website of Central Bank of Kenya", 22nd July 2013. https://news.softpedia.com/news/Gaza-Hackers-Deface-Website-of-Central-Bank-of-Kenya-369847.shtml. Last accessed 1st August 2020.

298. E. Kovacs, "Russia's Central Bank and other financial institutions hit by DDOS Attacks", 18th October 2013. https://news.softpedia.com/news/Russia-s-Central-Bank-and-Other-Financial-Institutions-Hit-by-DDOS-Attacks-392528.shtml. Last accessed 1st August 2020.

299. E. Kovacs, "Three Lloyds clerks used hacking device to steal money from customer accounts", 24th April 2014. https://news.softpedia.com/news/Three-Lloyds-TSB-Clerks-Used-Hacking-Device-to-Steal-Money-from-Customer-Accounts-439202.shtml. Last accessed 1st August 2020.

300. E. Kovacs, "Turkmenbashi and PrezidentBank State Commercial Banks of Turkmenistan hacked", 7th February 2014. https://news.softpedia.com/news/Turkmenbashi-and-PrezidentBank-State-Commercial-Banks-of-Turkmenistan-Hacked-424965.shtml. Last accessed 1st August 2020.

301. Krebs on Security, "DDoS Attack on Bank Hid $900,000 Cyberheist", 13th February 2013. https://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist. Last accessed 1st August 2020.

302. Krebs on Security, "Feds charge Calif. brothers in cyberheists", 13th November 2014. https://krebsonsecurity.com/2013/11/feds-charge-calif-brothers-in-cyberheists. Last accessed 1st August 2020.

303. Krebs on Security, "Hacker ring stole 160 million credit cards", 25th July 2013. https://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/. Last accessed 1st August 2020.

304. Krebs on Security, "Thieves Jam Up Smucker's, Card Processor", 4th March 2014. https://krebsonsecurity.com/2014/03/thieves-jam-up-smuckers-card-processor. Last accessed 1st August 2020.

305. KXII, "Durant PD issues warrants for Romanian duo in credit card fraud case", 12th February 2016. No longer available online. Last accessed 5th December 2019.

306. Local10, "Chase Bank teller arrested in connection with Miami Beach skimming scam", 11th October 2017. https://www.local10.com/news/2017/10/11/chase-bank-teller-arrested-in-connection-with-miami-beach-skimming-scam/. Last accessed 1st August 2020.

307. MassLive, "ATM 'skimmer' admits ripping off $121,000 from TD Bank customers in 5 Western Massachusetts communities", 14th October 2015. https://www.masslive.com/news/2015/10/atm_skimmer_pleads_guilty_in_s.html. Last accessed 1st August 2020.

308. M.P. Mayko, "Man pleads guilty to ATM-skimming thefts", 29th August 2013. https://www.stamfordadvocate.com/local/article/Man-pleads-guilty-to-ATM-skimming-thefts-4744611.php. Last accessed 1st August 2020.

309. N. McBride, "Kiwibank apologises after privacy breach", 11th October 2013. https://www.nzherald.co.nz/business/news/article.cfm?c_id=3\&objectid=11138757. Last accessed 1st August 2020.

310. J.P. Mello Jr., "Anonymous posts personal data of 4,000 bankers online", 5th February 2013. No longer available online. Last accessed 5th December 2019.

311. J. Melvin, "Wells Fargo teller stole $119,000 from elderly customer", 16th August 2013. https://www.mercurynews.com/2013/08/16/wells-fargo-teller-stole-119000-from-elderly-customer-da-says. Last accessed 1st August 2020.

312. NJ Today, "NY man pleads guilty to role in ATM skimming scheme", 10th September 2013. http://njtoday.net/2013/09/10/ny-man-pleads-guilty-to-role-in-atm-skimming-scheme. Last accessed 1st August 2020.

313. Office of the Privacy Commissioner (New Zealand), "Case note 203856 [2009] NZPrivCmr 12: Bank teller improperly accesses customer account information", 4th May 2009. https://www.privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-203856-2009-nzprivcmr-12-bank-teller-improperly-accesses-customer-account-information. Last accessed 1st August 2020.

314. Patch.com, "Accused ATM skimmers plead not guilty", 21st March 2014. No longer available online. Last accessed 5th December 2019.

315. J. Patterson, "Romania arrests three for stealing client information from Cypriot brokerage", 20th July 2017. https://www.financemagnates.com/forex/regulation/romanian-authorities-apprehend-three-men-trying-sell-stolen-client-data. Last accessed 1st August 2020.

316. Reuters, "Ex-Goldman Sachs boss jailed for information leak", 18th June 2014. https://www.dailysabah.com/americas/2014/06/18/exgoldman-sachs-boss-jailed-for-information-leak. Last accessed 1st August 2020.

317. E. Rosenfeld, J. Cox and M. Thompson, "Morgan Stanley: An employee stole partial client data", 5th January 2015. https://www.cnbc.com/2015/01/05/morgan-stanley-an-employee-stole-partial-client-data.html. Last accessed 1st August 2020.

318. J. Rowbotham, "Three arrested on ATM scam charges", 20th December 2013. https://www.dailyrecord.co.uk/news/local-news/three-men-arrested-west-stirlingshire-2945395. Last accessed 1st August 2020.

319. Rubin Thomlinson, "Privacy breach by employee could have price tag for employer", 4th July 2014. https://rubinthomlinson.com/privacy-breach-employee-price-tag-employer. Last accessed 1st August 2020.

320. T. Samson, "Hacker group demands 'idiot tax' from payday lender", 20 June 2012. https://www.infoworld.com/article/2617597/hacker-group-demands--idiot-tax--from-payday-lender.html. Last accessed 1st August 2020.

321. R. Schiavone, "Man admits installing skimming device in La Quinta ATM in plea deal", 22nd July 2013. https://patch.com/california/palmdesert/man-admits-installing-skimming-device-in-la-quinta-atm-in-plea-deal. Last accessed 1st August 2020.

322. R. Schiavone, "Police: man installs skimming devices in La Quinta ATM, tries to use stolen info in Palm Desert", 16th March 2013. https://patch.com/california/palmdesert/police-man-installs-skimming-devices-in-la-quinta-atm-tries-to-use-stolen-info-in-palm-desert. Last accessed 1st August 2020.

323. The Signal, "2 suspected gang members arrested in computer theft", 8th May 2013. No longer available online. Last accessed 5th December 2019.

324. S. Sirletti and E. Robinson, "Hackers breach 400,000 UniCredit Bank accounts for data", 26th July 2017. https://www.bloomberg.com/news/articles/2017-07-26/unicredit-says-400-000-clients-affected-by-security-breach. Last accessed 1st August 2020.

325. Spamfighter, "Hackers compromising and blackmailing Indian pharma companies and banks", 18th January 2016. http://www.spamfighter.com/News-20054-Hackers-Compromising-and-Blackmailing-Indian-Pharma-Companies-and-Banks.htm. Last accessed 1st August 2020.

326. Threatpost, "Anatomy of the RBS WorldPay Hack", 10th November 2009. https://threatpost.com/anatomy-rbs-worldpay-hack-111009/73073. Last accessed 1st August 2020.

327. ThreatPost, "Feds bust cybercrime ring targeting payroll, financial firms", 22nd June 2013. https://threatpost.com/feds-bust-cybercrime-ring-targeting-payroll-financial-firms/100962. Last accessed 1st August 2020.

328. M. Udland, "A hedge fund was hacked in a never-before-seen attack", 19th June 2014. https://www.businessinsider.com/hedge-fund-hacked-in-complex-attack-2014-6. Last accessed 1st August 2020.

329. The United States Attorney's Office — District of New Jersey, "Eight Charged With Fraud, ID Theft, Money Laundering In Multimillion-Dollar International Cybercrime Scheme", 12th June 2013. https://www.justice.gov/usao-nj/pr/eight-charged-fraud-id-theft-money-laundering-multimillion-dollar-international. Last accessed 1st August 2020.

330. WBTV, "Feds: Man arrested in Charlotte for skimming part of larger conspiracy", 4th June 2015. https://www.wbtv.com/story/29243112/feds-man-arrested-in-charlotte-for-skimming-part-of-larger-conspiracy. Last accessed 1st August 2020.

331. C. Weston, "No end in sight to Ulster Bank problems causing chaos for customers", 3rd July 2012. https://www.independent.ie/business/irish/no-end-in-sight-to-ulster-bank-problems-causing-chaos-for-customers-26871744.html. Last accessed 1st August 2020.

C

Participant Information Sheet — Survey

Introducing attacker personas: professional perception and practical potential — a digital banking perspective (survey information sheet)

Caroline Moeckel (PhD candidate), Dr Geraint Price (academic supervisor)
Royal Holloway, University of London

The research problem

Personas as an archetypical representation of non-malicious users have been traditionally used to represent a range of legitimate and task-driven system users in user-centred design and digital settings. The potential usefulness of persona representations in alternative settings, for example in information security, has been recognised by several authors in the past in a largely academic context (e.g. Atzeni et al., 2011; Bødker and Klokmose, 2013; Steele and Jia, 2008).

However, practical uptake in organisations by practitioners in areas such as digital, fraud, risk and security (or mixed agile teams) seems limited at this point in time. To date, methodological advancement for attacker personas and interest from security practitioners for attacker personas have been sparse and very little end-to-end examples of attacker personas have been built and presented for real-life applications. This may be due to a lack of perceived value, usefulness or practical context, but could also be due to a shortage of skills to build meaningful attacker personas in an organisation.

This is in strong contrast to the relatively widespread use of user personas in disciplines like marketing or digital. To help define reasons behind this disparity and potentially define further research directions in this area, this research aims to investigate the perception of attacker personas by practitioners in organisations (using the example of financial services and digital banking specifically).

Further background

There are many ways of building personas, with varying levels of formality, effort and detail involved in both the commercial and academic space. For the specific purpose of building attacker personas in this work, an approach with relatively high levels of formality and guidance to ensure potential replicability, adaptation and extension of the method was required. The relative lack of mature methods for attacker personas specifically meant that a user persona creation method from user-

centred design seemed to be a good choice, although some adaptations for attacker personas would have to be made. Based on reasoning presented in this introduction, an adapted version of the process model proposed by Nielsen in her work (2013) is used. Nielsen's framework is especially compelling as it provides a relatively formal, sequential approach to persona building, while incorporating other key works and authors in the area.

Lastly, from a conceptual point of view, the role that attackers as human adversaries play in security modelling does not seem to be fully defined at this point in time. Attacker-centric threat modelling is contested in Shostack (2014), raising the overall question where, how and why attacker representations fit into the wider security management process.

Participant information
Thanks for agreeing to support this research. In line with the requirements for ethical procedures for academic research undertaken by UK institutions, information on participation and how information obtained will be used should be provided. For this small-scale research project and the survey shared with you, please be aware of the following points:

- All results collected through the survey are anonymous and the link shared is not attributed to individual participants.
- Therefore, once answers have been submitted through the survey link, withdrawal or deletion of answers provided is generally not possible as all results are recorded on an anonymous basis and can't be distinguished from each other.
- Access to these notes/emails is limited to the researcher/supervisor.
- Summary results may be used in the PhD thesis of the researcher and subsequent academic publications/papers deriving from this.
- While information gained during the study may be published, all summary content will be fully anonymised to ensure neither participants, their organisations or employers can be identified.
- An ethical review process has been completed following the guidelines on ethical approval for research projects from Royal Holloway, University of London (*rhul.ac.uk*).
- Researchers may be contacted for any questions:
  Caroline Moeckel, *caroline.moeckel.2012@live.rhul.ac.uk, +44 75 38481636*
  Dr Geraint Price, *geraint.price@rhul.ac.uk, +44 1784 414160*

Sources

- Andrea Atzeni, Shamal Faily, John Lyle, Cesare Cameroni and Ivan Fléchais. 2011. Here's Johnny: A methodology for developing attacker personas. Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security (ARES'11), Vienna, Austria, 22–26nd of August, 2011. pp.722–727.
- Bødker, Susanne and Klokmose, Clemens Nylandsted. 2013. From Persona to Techsona. Human-Computer Interaction – INTERACT 2013, Cape Town. pp. 342–349.
- Adam Steele and Xiaoping Jia. 2008. Adversary Centered Design: Threat Modeling Using Anti-Scenario. Proceedings of the 2008 International Conference on Information and Knowledge Engineering (IKE'08), Las Vegas, NV, US, 14–17th of July, 2008.
- Lene Nielsen. 2013. Personas — User-Centred Design. Springer, London.
- Adam Shostack. 2014. Threat Modeling: Designing for Security. Wiley.

D

Documentation/List of Questions — Survey

Introducing Attacker Personas in Financial Services — Survey Study
Sequencing and list of question statements

Introduction
Welcome & introduction, including researcher contact details

Background

- Which term (or multiple terms) describe your job role/level most accurately? Senior manager or executive / manager / analyst / specialist or subject matter expert / developer / designer / Other (please specify) / prefer not to say
- Which area (or multiple areas) do you identify with the most? Security (specifically: cyber security, physical security, corporate security) / fraud / risk / digital / business / consulting / other (please specify) / prefer not to say
- Have you come across the concept of Personas before? Yes / no
- And specifically, have you come across the concept of Attacker Personas (or other similar representations of human adversaries)? Yes / no

Meet the attacker personas...
Overview of attacker persona set
Example persona profiles (Bruno, Kev and Scott)

The following survey statements are scored against a 5-point Likert scale: strongly agree / agree / neither agree or diagree / disagree / strongly disagree.

Clarity of the personas

- The shown persona profiles were easy to read and understand.
- The short bio section for the personas was easy to read and understand.

- Seeing the complete persona set (the 7 different attacker profiles) was helpful and made sense.
- Overall, I enjoyed looking at the persona set and reading through the persona profiles.
- I understand what the persona method is trying to achieve.

Completeness & Consistency

- There is plenty of information on the individual personas.
- The profile pictures match the descriptions of the personas and represent them well.
- The personal data (like name and age) used in the profiles matches the descriptions of the personas and represents them well.
- The personas seemed very generic to me.
- Additional real-life situations and scenarios would have been useful.
- Additional information on how the personas may affect customers of this organisation (and their customer journeys) would have been useful.

Completeness & Consistency

- Some of these personas match attacker types I have heard of before (e.g. in the media).
- Some of these personas match attacker types I have heard of in an industry context.
- Some of these personas match attacker types I have come across in this organisation.
- I understand the motivations of the attacker portrayed by the personas.
- The personas could be real people and adversaries that actually exist.
- Overall, the personas included in the set seemed credible.

Relevance & Applicability

- I have learned something from reading through these profiles.
- I wish the personas were more tailored to my organisation or industry.
- I don't see practical value and applicability of this method to my organisation and job role.
- In my job role, I could use a persona set like the one shown or similar.

Usefulness & Willingness

- Overall, I found this persona set useful in understanding the potential adversary landscape to digital banking.
- Looking at this, I feel like this could be a useful tool for speaking to senior stakeholders in my organisation.
- It's something I could see value in for training or raising security awareness in my organisation.
- I feel like an attacker persona set using our own data could be useful for my work.
- I feel like an attacker persona set using our own data could be useful for others in my organisation.
- In the future, I would be interested in taking part in an exercise to create attacker personas specific to my organisation or work.

Other feedback (optional)

E

Participant Information Sheet — Interviews

The role of the attacker in information security and threat modelling – a digital banking perspective (information sheet)

Caroline Moeckel (PhD candidate), Dr Geraint Price (academic supervisor)
Royal Holloway, University of London

The research problem

Attacker profiling and other efforts to collect and present information about cybercriminals or malicious insiders have long been part of information security. However, using this information in security assessments and general risk management is not always easy in practice – essentially, knowing a lot about attackers doesn't necessarily make it easy to understand the threats they pose and their attacks. This is not to say that attacker information cannot add tangible benefits in a security context, but it is felt that more clarity needs to be gained to understand what these benefits currently are and what future opportunities can be identified. Using the example of financial services, a literature review on how information on attackers is used in current security practice is proposed. Additionally, it is felt that insights from practitioners in financial services on how they use such information (or perceive it to be used) will help to understand the current status quo and explore future directions the area.

Further background

Structured approaches on how knowledge on attackers is used in risk assessments and the overall security ecosystem of an organisation seem to be hard to find. Often, approaches focusing on attackers only serve as a supplement for other approaches (OWASP[95]) or information collected on attackers remains largely unused in the security assessment process (as it is not required by many tools or methods, e.g. Microsoft's Threat Modelling tool[96]). In his widely respected work on threat modelling,

[95]OWASP (2017), "Threat modeling OWASP pages", https://owaspsummit.org/working-sessions/ threat-model/threat-model-owasp-pages.html, June 2017

[96]Microsoft (2017), "What's new with Microsoft threat modelling tool", in Microsoft Secure Development blog, https://blogs.msdn.microsoft.com/secdevblog/2017/04/21/whats-new-withmicrosoft-threat-modeling-tool-preview, April 2017

a technique to think about threats to a system in a structured manner, Shostack[97] generally advises against using an attack-centric approach (meaning it focuses on finding threats by looking at the attackers applicable to a system). This is based in the assumption that knowledge about attackers will not enable the person conducting the threat modelling exercise to build a list of applicable threats very easily – attacker lists or personas for example do not offer enough structure to reliably identify related threats. Similarly, 'thinking like an attacker' is considered difficult and seen to attract personal biases from the person creating the model (also in Shostack).

Questions for discussion
Topic 1: What role do you currently see the attacker play in a security modelling and assessment context? In your experience, how is attacker information used in practice?
Topic 2: How does this role need to change to potentially provide better value?

Participant information
Thanks for agreeing to support this research. In line with the requirements for ethical procedures for academic research undertaken by UK institutions, information on participation and how information obtained will be used should be provided. For this small-scale research project, please be aware of the following points:

- Notes of our conversations/email records will be taken/used by the researcher.
- Access to these notes/emails is limited to the researcher/supervisor.
- Notes/emails will be stored securely on a corporate/university secured network, only until the thesis work is completed (end 2020 planned) and then deleted.
- Summary content or quotations from these conversations may be used in the PhD thesis of the researcher and subsequent academic publications/papers deriving from this.
- While information gained during the study may be published, all summary content or quotations will be fully anonymised to ensure neither the interviewee or its organisation or employer can be identified.
- A version of the summary content or quotations will be shared and consent in writing for inclusion in specific publications will be asked for at this point. All participants are able to withdraw (entirely or in parts) from this project at any point.
- An ethical review process has been completed following the guidelines on ethical approval for research projects from Royal Holloway, University of London (*rhul.ac.uk*).
- Researchers may be contacted for any questions:
  Caroline Moeckel, *caroline.moeckel.2012@live.rhul.ac.uk, +44 75 38481636*
  Dr Geraint Price, *geraint.price@rhul.ac.uk, +44 1784 414160*

[97] Shostack, Adam (2014, p.40), "Threat Modeling: Designing for Security", Wiley