Comparing Cyber Weapons to Traditional Weapons Through the Lens of Business Strategy Frameworks

by Nicola Bates

Supervisor: Professor Konstantinos Markantonakis

Information Security Group

Royal Holloway, University of London

Acknowledgements

My thanks go to Professor Konstantinos Markantonakis for supervision on this project.

Also to Dr Raja Naeem Akram for advice on where to focus analysis, Dr Michelle Bentley for discussion on weapon categorisation, Dr Nicholas Griffin for casting an eye over strategy framework use within this context, Dr Robert Bates for help on strategic framework analysis and Neil Ashdown for proof reading and feedback.

Table of Contents Page

Acknowledgements……2
List of figures and tables……6
Executive summary……8
1. Introduction and background……10
1.1 Introduction……10
1.2 What is a cyber weapon?……11
1.3 Cyber weapons considered for analysis……13
1.4 Actors in cyberspace……14
1.5 Overview of strategic frameworks……16
1.5.1 PESTLE……16
1.5.2 Porter's Five Forces……18
1.5.3 SWOT……19
1.6 Summary and methodology……20
2. Comparisons of cyber and conventional weapons……21
2.1 Introduction……21
2.2 The fifth domain of warfare……21
2.3 The battlefield……22
2.3.1 Reach……23
2.3.2 Speed……23
2.3.3 Volatility……23
2.3.4 Target dependence……24
2.3.5 Offence dominance……24
2.4 Under theorisation……25
2.5 Threat assessment……25
2.6 Attribution……26
2.7 Proliferation……27
2.8 Legal aspects……28

2.9 Cost……..29
2.10 Diversity of actors……..31
2.11 Life expectancy of weapons……..32
2.12 Intrusion and attack may look the same in cyber……..32
2.13 Improved defences counter attacks globally……..33
2.14 Conclusion……..34
3. PESTLE analysis of cyber and conventional weapons…..……35
3.1 Introduction to attacks…..……..35
3.2 Estonia – April 2007…..……36
3.3 Invasion of Georgia – August 2008…..……38
3.4 Stuxnet – June 2010…..……..……40
3.5 Saudi Aramco – August 2012…..……42
3.6 F-35 IP theft – 2013 …..……..……44
3.7 Sony Pictures – November 2014…..……46
3.8 Financial transactions, SWIFT – 2014-2015…..……48
3.9 Ukraine power grids – December 2015…..……..50
3.10 US election interference – November 2016…..……..……52
3.11 WannaCry – May 2017……..……54
3.12 Conclusion……55
4. Porter's Five Forces analysis……..……..57
4.1 Introduction……..…57
4.2 Threat of substitute products……57
4.3 Threat of protection versus attack……58
4.4 The power of buyers and the power of suppliers……...59
4.5 Rationality of the market……...61
4.6 Conclusion……62
5. Conclusions……...64
5.1 Conclusion……64
5.1.1 Cyber changes the battlefield……64
5.1.2 Areas where cyber is beneficial……65

5.1.3 Challenges of deploying cyberattacks ……66
5.1.4 Cyber weapons are here to stay……68
5.2 Further work……69
5.3 Closing thoughts……72
Appendices……...73
Appendix 1: PESTLE results for Estonia……..73
Appendix 2: PESTLE results for Georgia……..75
Appendix 3: PESTLE results for Stuxnet……...77
Appendix 4: PESTLE results for Saudi Aramco……..79
Appendix 5: PESTLE results for F-35 IP theft……..82
Appendix 6: PESTLE results for Sony Pictures……83
Appendix 7: PESTLE results for SWIFT……85
Appendix 8: PESTLE results for Ukraine power……...87
Appendix 9: PESTLE results for US election……..89
Appendix 10: PESTLE results for WannaCry……...91
List of definitions and acronyms……..94
References……95

List of tables and figures Page

Table 1: Relationship between state and non-state actors in cyberattack……..14
Table 2: Types of threat actors in the cyber domain ……..……15
Table 3: PESTLE analysis descriptions for cyber weapons comparison…..……..17
Table 4: Porter's Five Forces descriptions for competitive market analysis……19
Table 5: Comparison of the five domains of warfare.……22
Table 6: Summary PESTLE analysis for Estonia..…..……..……...38
Table 7: Summary PESTLE analysis for Georgia...……..……..39
Table 8: Summary PESTLE analysis for Stuxnet……..……..……...42
Table 9: Summary PESTLE analysis for Saudi Aramco……..……..44
Table 10: Summary PESTLE analysis for F-35 IP theft...……..……45
Table 11: Summary PESTLE analysis for Sony Pictures..……..……..48
Table 12: Summary PESTLE analysis for SWIFT……..……...50
Table 13: Summary PESTLE analysis for Ukraine power……..……..….52
Table 14: Summary PESTLE analysis for US election..……..……..54
Table 15: Summary PESTLE analysis for WannaCry..……..……55
Table 16: Combined PESTLE analysis……..……...56
Table 17: Summary of Porter's Five Forces analysis……...……63
Table 18: PESTLE analysis for Estonia...……..……...75
Table 19: PESTLE analysis for Georgia...……..……..77
Table 20: PESTLE analysis for Stuxnet..……..……...79
Table 21: PESTLE analysis for Saudi Aramco..……..……81
Table 22: PESTLE analysis for F-35 IP theft...……..……..83
Table 23: PESTLE analysis for Sony Pictures...……..……85
Table 24: PESTLE analysis for SWIFT...……..……87
Table 25: PESTLE analysis for Ukraine power……..……..……...89
Table 26: PESTLE analysis for election interference..……..……91
Table 27: PESTLE analysis for WannaCry..……..……..……27

List of tables and figures (continued) Page

Figure 1: Types of cyberattack……12

Figure 2: Cyberattacks considered in this report……..14

Figure 3: ZERODIM payouts for mobile phones……..30

Figure 4: Cyberattacks considered mapped to section numbers……..…..35

Executive Summary

Advances in technology have changed the way nation states conduct offensive operations, with cyber capabilities increasingly being used. With such rapid change it has been noted that more research is now needed into how the cyber domain fits into general strategic theory [1].

Traditionally this would be performed from a military perspective by looking at the direct comparison to kinetic means in terms of physical impact. With cyber weapons possessing a different set of characteristics, deployment and impact mechanisms, this report will propose, and demonstrate, that the application of business strategy methodologies to provide a suitable and insightful framework in which to consider the differences between cyber and kinetic attacks. Such frameworks can be used to explain the power dynamics between different actors within the cyber domain. The data from this work can then be used to analyse trends within operations using cyber weapons and conventional weapons in order to support decision making.

Within the current body of work the use of business strategy frameworks specifically for cyber weapons have only been found in consultancy companies, such as Inkwood Research [2], rather than in research papers or governments. Consultancy sources require payment to access and so have not been viewed. Comparing results to my research were therefore not possible.

This project aims to:

- increase knowledge of the cyber domain required for strategic decisions making;
- compare cyber and kinetic attacks which would achieve the same effect or objective;
- determine what the strategic benefits of cyber weapons are compared to traditional attacks, as well as the limitations and challenges of cyber weapons.

Historical examples of cyber weapons will be analysed using business strategy frameworks. These examples will be compared with alternative ways of achieving the same effect or objective using ‘traditional’ kinetic means and operations.

A market overview of the cyber weapons field will also be completed ranging from low end, downloadable tools, up to very sophisticated, targeted capabilities. This will provide a clearer understanding of how the cyber weapons market operates.

Key findings from analysis have been that cyber weapons:

- can combine action at a distance, with close quarters accuracy and efficiency, permitting a new class of attacks which are de-risked versus conventional means;
- offer the ability to strike rapidly, without warning across an entire network, propagating faster than investigators can react;
- In the main have reversible effects and are limited in duration allowing attacks to be used for signalling, to disrupt but not destroy infrastructure;

- are most effective when they augment kinetic capabilities offering a new, wider reaching and crucially deniable means of carrying out these activities;
- offer the ability to reach out and conduct influence operations faster and cheaper than would otherwise be possible to do without cyberspace.

Governments face difficult choices between exposing vulnerabilities or exploiting them to conduct cyber operations. There are also well-established challenges around attribution in the cyber domain. Taken together, these dynamics suggest that material changes in how governments approach international relations and national security are required. Additionally, with the increasing dependence on cyber systems for core day-to-day functions (communications, finance, health) the ability of attackers to target those areas which have been viewed as ‘off-limits’ in war has increased exponentially in recent years. This implies a need for new international rules and treaties to protect modern societies globally.

‘The growth of cyber arsenals, in short, is outpacing the design of doctrines to limit their risk [3, p. 3].’

1. Introduction and background

1.1 Introduction

It was Sun Tzu who said ‘The supreme art of war is to subdue the enemy without fighting [4].’ While Sun Tzu could not have anticipated the technological environment of the 21st century, he would surely have been fascinated and terrified by the possibilities it presents for subduing an opponent without open conflict. For those abilities frequently referred to in the Art of War – subtlety of movements, mysteriousness of actions, dominance through strategy and the ability to predict and misguide an opponent – are more evident and achievable within the cyber domain than they ever were in a conventional setting.

In 2009 the US government setting up a Cyber Command tasked with dealing with cyber conflicts, with a new domain of ‘cyberspace’ officially incorporated into doctrine in 2011 [5]. Just a few years later, in 2017, the Director of the NSA and US Cyber Command stated that ‘every conflict around the world now has a cyber dimension [6].’

During these years, armed forces have realised that to stay competitive in this digital realm they will need to become cyber enabled and capable.

With a lack of cyber knowledge amongst military and political leadership countries are struggling to make sense of what is involved in meeting this requirement and how they should organise. For most this remains an open question. Despite weapons technologies advancing significantly, with unmanned and autonomous vehicles and increasingly precise guided munitions, the general principles of war remained constant. These are to know the enemy, know where to strike and where to defend, and control the narrative - with the ability to perform any of these becoming far more complex within the cyber arena.

At a strategic level, governments are struggling to combine traditional armed force capabilities, other instruments of national power and the new cyber weapons [1]. North Atlantic Treaty Organisation (NATO) officially recognised cyberspace as the fifth domain at the 2016 Warsaw summit, allowing a cyberattack on a NATO member state to activate Article 5 of the treaty [7]. This allows for the alliance to respond with conventional weapons, the severity of which would depend on the cyberattack.

However, merely arriving at a definition of what constitutes cyberwar is controversial and full of disagreements, with books and papers within international relations and security studies arguing cyber war will or will not even happen [8], [9]. This particular controversy has been avoided by focussing instead on the area of cyber weapons.

Even this is a controversial subject, with a similar quagmire of disagreement over any definition. However, after a brief description of what countries in the East and West understand as constituting a cyber weapon, what will be considering a cyber weapon for the purposes of this report will be defined.

Within the cyber domain matters are further complicated by the variety of actors operating in this space, in contrast to the traditional focus on nation-states in international relations. Indeed in assessing the earliest cyberattacks governments

were struggling to differentiate teenage pranksters from large nation states. Given the variety of actors in this space, these will be summarised to clarify which groups are being discussed and analysed within this project.

The strategic frameworks I will be considering will be PESTLE, Porter's Five Forces and a SWOT analysis. Although these are traditionally used in a business strategy setting, they provide a clear method in which to make comparisons between cyberattacks and traditional attacks. My focus will be on the effects the cyberattack was trying to achieve (as well as the realised effects, if different), in comparison to the traditional ways of achieving those effects.

1.2 What is a cyber weapon?

There is much discussion in the literature as to the precise meaning of the term 'cyber weapon', with no consensus on a final definition. I will therefore start by describing some of these definitions before setting out my own working definition.

It is useful to start with the technical factors before moving onto what use cases will be deemed to fall under the criteria required of a cyber weapon. A cyber weapon relies on the combination of three things [10].

1. A vulnerability (penetration mechanism): For example, a weakness or design flaw in a hardware or software component that can be manipulated by an attacker, allowing the weapon to obtain access to the system under attack. The vast majority of attacks use well-known vulnerabilities, including those for which patches have been released. Some, however, use zero-day vulnerabilities which have not been disclosed to the vendor for a patch.
2. An exploit: Code which is written to cause a specific effect through taking advantage of a vulnerability. This could be gaining access to a system, exfiltrating information, disrupting communications or causing hardware to fail.
3. A propagation method: The way in which the exploit is delivered to a target, such as a phishing email or USB drive.

The weaponization aspect depends on the quality of intelligence gathered in other operations in order to identify and develop vulnerabilities, exploits, and propagation methods which would be the most promising for the system.

Some definitions use different terminology for data exfiltration (cyber exploitation) and if the payload causes damage, destruction, degradation or denial of use (cyberattack). I will be calling both of these effects a cyberattack and it will be obvious from the situation what the attacker is doing.

Cyberattacks vary depending on the effects they are trying to accomplish. Distributed Denial of Service (DDoS) attacks for example rely on overloading computer systems with huge volumes of data, sometimes using other machines that have been compromised by the attacker – so called 'zombie machines'. The vulnerability here is the inability of the system to respond to the volume of requests. Other types of cyberattack are shown in Figure 1.

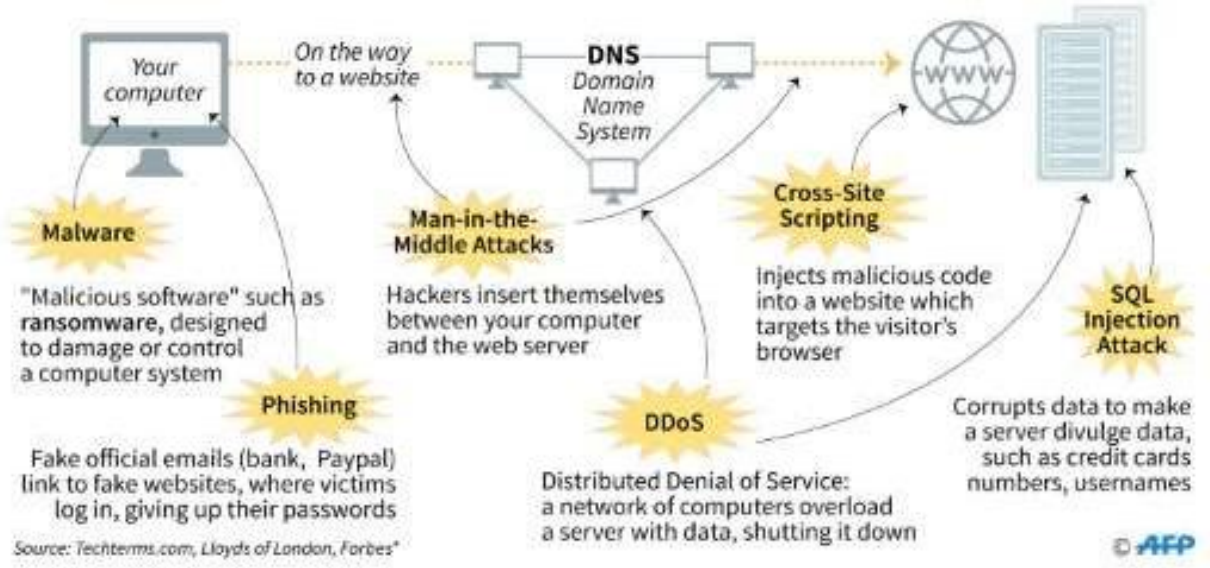

Figure 1: Types of cyberattack [11]

Countries in the West seem more interested in defining cyber weapons in terms of their destructive effects. This may stem from the influence of military strategist Von Clausewitz. Such definitions look something like, ‘A cyber weapon is a software-based Information Technology (IT) artefact or tool that can cause destructive, damaging, or degrading effects on the system or network against which it is directed [12].’ Such a definition would exclude the role that cyber weapons can play in operations aimed at exfiltrating information, for example.

However, when we look to the East a fuller range of options spring up from soft to hard power, with writings on this subject emphasising dominance through tactics and skill rather than brute force, and taking an enemies assets without destroying them [4]. As such, many events which incorporate information theft, social manipulation and disruption achievable through cyber equally deserving of the label ‘weapon’ or ‘attack’. Looking to Russia, military analyst Charles Bartles argues that Russia considers non-military attacks to be part of war, whilst the West views them as ways of avoiding war [13, p. 162].

An updated insight into the thinking of China’s military was released in February 1999, a book called ‘Unrestricted Warfare’ which broadened the definition of war beyond battlefield dominance [14]. The authors suggested that war no longer meant ‘using armed force to compel the enemy to submit to one's will’ but instead ‘using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests’ stating that ‘non-war actions may be the new factors constituting future warfare [14, p. 6-7]. Cyber weapons clearly have a part to play in such a broad conception of warfare.

1.3 Cyber weapons considered for analysis

For the purposes of this report, I will categorise cyber weapons by their intended effect. This can be either an enabler for another event, a means of causing political effects, or a means of affecting the physical world.

1. Enable: These would be espionage operations covering intelligence collection and preparation of the battlefield using cyber means. This would enable further operations with other components such as traditional kinetic means.

2. Political: These are operations to influence others, control the political environment, or dictate the narrative. This could range from the soft power of propaganda, through to the hard power of coercion through the threat of leaking hacked information.

3. Physical: Attacks which have a physical manifestation to various degrees of severity, categorised as:
   - annoyance, low-level disruption and embarrassment such as altering connected lighting devices;
   - destabilisation and confusion to show power and intent, such as failure in a national power grid;
   - force which causes permanent physical damage to equipment or humans such, such as an attack on a nuclear plant.

The use of cyber to acquire information for espionage purposes and enablement alone will not be considered as a cyberattack. Rather, I argue that this falls under the umbrella of espionage which has existed for millennia and is considered by countries to be part of the international landscape [15]. Nonetheless, it is worth noting that nearly all cyberattacks will have an intelligence component, for example in enumerating the target network.

Propaganda used to be expensive and time consuming, with the ability to control mass media such as television and newspapers generally limited to nation-states. With ubiquitous internet connections and social media accounts open to all, the present ability to precision target a message is very effective and can cause political volatility. These attacks will therefore be included in analysis.

Low-level physical attacks will not be considered unless they form a part of another more impactful cyberattack – such as power grid failure as well as website defacement – with the main focus on the higher physical impact. Cyberattacks causing political destabilisation and physical damage will form part of the definition of a cyber weapon for the purpose of this report.

Having established my definition of ‘cyber weapon’, I will now review a range of historical cyberattacks over time, with a focus on the effect the use of the cyber weapon was intended to achieve.

The choice of attacks was shaped by the limited information available in open sources on some attacks. Moreover, I have avoided consideration of more recent attacks, where less information on attribution and attack techniques are available.

This process resulted in ten examples being selected, shown in chronological order in Figure 2. Ten were chosen to provide enough material to bring out relevant findings without encountering excessive repetition.

Figure 2: Cyberattacks considered in this report

Two attacks I have not included in the sample – but which are nonetheless interesting – are the Sands Casino attack and the NotPetya attack on Ukraine.

The Sands Casino cyberattack in February 2014 was attributed to Iran and targeted a Las Vegas casino [15, p. 161]. I felt this had very similar attributes to the Sony attack included in my sample, not only in that it targeted a private company based in the United States (US) but also in that it had the goal of trying to stifle free speech. Moreover, Iran as an aggressor, and victim, has been covered in other examples chosen already.

The NotPetya attack is still the most damaging and expensive cyberattack in history [16], but I excluded this due to the similarity with the Saudi Aramco attack. Both attacks targeted a nation state, but in both cases the main victim was a large corporation (in the case of NotPetya the shipping company Maersk). Moreover, Russia was already well represented as a likely attacker in my sample.

1.4 Actors in cyberspace

It is useful to have a breakdown of the various actors in cyber space, given they have different objectives, capabilities and ways of doing things. A simple split would be between state and non-state actors acting as an attacker or defender, as noted in Table 1.

		Attacker	
		State	Private
Defender	State	One state targets another state's strategic computer assets, e.g. Stuxnet	Militant group or patriotic hackers target a foreign states computer assets, e.g. Estonia
	Private	A state attacks private computers within another state for strategic or commercial reasons, e.g. Sony Pictures	Exchange of blows among nonstate entities e.g. Anonymous against Islamic State

Table 1: Relationship between state and non-state actors in cyberattacks [3, p. 183]

It is useful to break the non-state actors down further given the range of actors encompassed in this category. Criminals for example will usually be quite indiscriminate as to their specific target so long as there is money to be made. They will go after the 'low hanging fruit', moving on if a system is too well protected. A hacktivist on the other hand is more likely to be politically motivated to attack a particular set of targets.

A government attacker on the other hand will have been given orders and will keep on trying until the mission is either achieved, be that weeks, months or years, or until they are detected. Usually a government target will be for political gains but reports suggest that some countries, for example North Korea, have engaged in cyber operations for financial gains [17].

When an attacker has a more sophisticated way of operating and will not give up no matter the high defences and time taken then these are usually named Advanced Persistent Threats (APT's). Knowing the attacker tools, syntax in code, motivations and persistence helps detection and attribution for example.

Actors	Motives	Activities	Targets	Resources
Nation State	Political / Economic	Espionage, influence operations, reconnaissance, infrastructure	Nation states, terrorists, hacktivists, organised crime	High, variable skill sets, use black markets
Terrorists	Political / Economic	Infrastructure, extortion, social media, targets causing panic/disruption	Nation states	Limited, low expertise
Hacktivists	Political	Depends on beliefs, e.g. environment, target oil/gas companies disrupt operations	Nation states, political parties, companies	Low to high skill level, use black markets
Organised crime	Financial	Hijacked resources, fraud, intellectual property theft, Illicit content, scams, crime for hire	Individuals, banks, businesses	Mobilising cyber-crime networks, professional, uses black market
Criminals	Financial	Fraud, intellectual property theft, scams	'low hanging fruit' of the internet	Use black markets,
Individual actor/script kiddies	Financial / kudos	IP theft, DoS attacks, defacing websites, blackmail	Likely to be instructed or be random attacks	Lack of funding and resources, reliant on 'plug and play' tools

Table 2: Types of threat actors in the cyber domain [18, p. 19]

A breakdown of the main actors in the cyber domain is given in Table 2. Of note here is that the definition of nation states includes non-state actors if it is highly likely that these are under state control. Possible examples would include Estonia's Cyber Defence League and various Russian cyber militia hackers.

The ten attacks chosen mainly focus on the actions of nation states, with the protagonists being Russia, Iran, North Korea, China, US and Israel. The victim of most of the attacks are the Ukraine, with the US and private companies targeted in two cases , and the UK and Iran in one case each.

Script kiddies feature heavily in one attack, namely in the cyberattack on Estonia in 2007. Terrorists, hacktivists, organised crime and other criminals do not feature in the examples chosen, although in some respects, North Korea's actions in cyberspace resemble organised criminality.

1.5 Overview of strategic frameworks

Strategy is the long term direction of an organisation including its goals, scope of activities and the capabilities it brings. Competitive strategy is the search for superior performance relative to competitors and identifying the investment trade-offs to deliver this. 'A strategy that is well thought out should bring about long-term success using creative actions that are hard for others to recreate [19].'

Strategy means different things to different people. It cannot be condensed to one thing but includes goals, objectives, planning and resources. Strategic development utilises the identification of core challenges to find out current positioning and is mainly linked to the external environment and the impact of decisions made.

There are three main ways in which to perform analysis on an industry sector:

1. PESTLE analysis: Used to analyse the macro environmental factors (the external factors);
2. Porter's Five Forces: The competitive forces model;
3. Strength, Weaknesses, Opportunities, Threats (SWOT) analysis.

Rather than applying these frameworks to a business setting I will use these to compare the different strategic considerations arising from how the effects of the selected attacks could have been achieved using conventional weapons in order to discover the strategic benefits of the cyber arena.

These frameworks will now be described further with the specific information needed in which to analyse weapons within the areas discussed.

1.5.1 PESTLE

The PESTLE framework considers important external issues influencing strategy.

It acts as a checklist, being a simple - and consistent - way to categorise and analyse the external global environment into six key types: political, economic, socio-cultural, technological, legal and environmental.

Depending upon the type of strategy being developed, the relative importance of each category can be weighted, with critical success criteria (and catastrophic failures) identified. Table 3 sets out the framework for a PESTLE analysis of a cyberattack.

Political	• Political factors at a local, regional and national level – both within the attacking and target countries • The impact of the attack on: stability, political capital, population unrest, elections, treaty discussions, sanctions, UN involvement • Macro risk (attaching to whole countries) and micro risk (attaching to specific organisations)
Economic	• Economic factors at a local, regional and national level • The cost of the weapon(s), systems, training, personnel, contractors • The cost of the impact to the target
Social-cultural	• Impact upon the professional and/or personal life as well as behaviours and habits • Cultural change, unrest, destabilisation, psychological distress, anxiety, distrust, loss of income
Technological	• Technological advances, developments and adoption • Does the technology exist to perform the attack, how cutting edge (or generic) is the technology, is it easily accessible • How feasible is the attack, taking into account the capabilities of the threat actor
Legal	• Legislation and regulations at a national and global level • The rules of war governing armed conflict, the Tallinn Manual 2.0 for cyber operations, NATO collective response and UN sanctions • Laws in relation to IP rights, election spending, trade deals, competition laws
Environmental	• Environmental issues at a local, national and global level • Pollution, waste production, waste disposal and climate change

Table 3: PESTLE analysis for cyber weapons comparison [19]

Factors will be specifically identified which are important to the weapons used and their impact within the environment and attack under examination. The data from this work can then be used to analyse trends within operations using cyber weapons and conventional weapons in order to support the points of difference between them.

The scenarios chosen are actual cyberattacks, meaning that we can draw plausible conclusions as to how cyber weapons will be used in the future. A range of usage scenarios are given to explore and evaluate future strategic possibilities. The main goal of performing a PESTLE analysis is to identify opportunities and threats.

1.5.2 Porter's Five Forces

The Porter's Five Forces model helps businesses identify the attractiveness of industries and markets and to identify their potential for change. This provides an understanding of the company's position relative to other players in the industry. It helps identify opportunities and threats in the environment to assist with planning.

Within the context of this project the model will be used to analyse the underlying markets for cyber weapons in order to determine how the creation of different attacks is impacted by competitive forces. Porter's considers each of the key areas required to develop, perform and sustain capabilities – their availability, level of skills required, powers of the actors to meet the goals and the issues of buyer and supplier powers.

At first glance, some of these may seem irrelevant – there being a limited number of people capable of designing and performing advanced cyberattacks, for example. However, closer inspection reveals that with few sanctioned areas in which to perform such actions the state has greater power within this area than may initially appear. This will become apparent within analysis, an overview of which is given in Table 4.

Porter's will be applied to the same cyberattacks analysed in the PESTLE framework rather than the entirety of the cyber weapons market. This gives more targeted cases to analyse given the huge diversity of capabilities and uses which fall under the definition of cyber weapons noted in Sections 1.2 and 1.3.

The Porter's analysis will be limited to cyberattacks only rather than the traditional weapon comparisons. As an established practice and with attacks common across many of the example, Porter's-based analyses of the kinetic defence industry will already exist within the wider literature.

Threat of substitute products	Substitutes are products and services that offer a similar benefit to an industry, but have a different nature. Customers will switch to alternatives and thus the threat increases if: • The price/performance ratio of the substitute is superior (e.g. aluminium more expensive than steel but more cost efficient for cars) • The substitute benefits from an innovation that improves customer satisfaction (e.g. trains can be quicker than aeroplanes on short haul routes) • The market is maturing or declining Examples of substitute product for cyber weapons would be various types of conventional weapons and propaganda outlets
Threat of new entrants	Threat of entry is low when conditions needed to be overcome to enter a market are high. The main barriers to entry are: - Economics of scale/high fixed costs - Experience and learning - Access to supply and distribution channels - Differentiation and market penetration costs - Legislation or government restrictions (e.g. licencing) - Expected retaliation from incumbents For cyber weapons new entrant threats would be from various actors, as described in Section 1.4

Power of suppliers	Suppliers provide organisation with things they need to produce their item or service. Supplier power is likely to be high when: • The suppliers are concentrated (there are few of them) • Suppliers provide a specialist or rare input • Switching costs are high (it disruptive or expensive to change supplier) • Suppliers can integrate forwards (e.g. low cost airlines have cut out the use of travel agents) In cyber weapons supplier power can come from price and exclusivity
Power of buyers	Buyers are the organisations immediate customers. If buyers are powerful, then they can demand cheap prices or product/service improvements. Buying power is likely to be high when: • Buyers are concentrated • Buyers have low switching costs • Buyers can supply their own inputs (backward vertical integration) In cyber weapons buyer power can come from price and exclusivity
Rationality of market	Competitive rivals have similar products and services and are direct competitors. The degree of rivalry increases hence rationality of the market decreases when: • Competitors have roughly equal size • Competitors are aggressive in seeking leadership • The market is mature or declining • The exit barriers are high • There is a low level of differentiation For cyber weapons, political tension and price inflation are the main factors to analyse

Table 4: Porter's Five Forces descriptions for competitive market analysis [19]

1.5.3 SWOT

The SWOT framework is a simple tool to force consideration of what the strengths, weaknesses, opportunities and threats for a particular organisation, strategy or course of action. It is useful for projects or market conditions but is less suitable for this analysis of cyber weapons, as I am looking to analyse a market rather than an individual competitor.

The SWOT analysis will therefore be incorporated into the PESTLE framework with the rating of the attacks regarding the best and worst options across categories being compared.

The SWOT analysis will further be utilised within the conclusion section where it will be used to pull out important findings from the PESTLE and Porter's five Forces analysis.

1.6 Summary and methodology

A cyber weapon is made up of three components, a vulnerability, an exploit and a way of propagation method. I have categorised cyber weapons by the effect they intend to achieve. Cyber weapons which produce political change, or cause disruption or physical damage will be considered in analysis by specifically focussing on ten examples chosen.

Malicious actors within these attacks are mainly confined to that of a nation state level, however, script kiddies also appear. Defenders include nation states, private companies and civilians.

Cyberattacks will be analysed using the PESTLE and Porter's Five Forces frameworks. For the PESTLE framework, each of the ten cyberattacks will be compared to two approaches, one of low kinetic effect and one of high kinetic effect, that could achieve the same impact using conventional means. For example, the Stuxnet cyberattack is compared with a special operations mission (low kinetic effect) and a conventional airstrike (high kinetic effect) which will have had a comparable impact.

The Porter's Five Forces framework will then be used to review the development of the attacks. Attacks will be considered together to identify the different competitive forces which would ultimately determine if a cyberweapons were the most efficient and economical way of achieving the intended effect.

2. Comparisons of cyber and conventional weapons

2.1 Introduction

Cyber weapons can possess unique features which make them desirable, such as the ability to cause damage falling short of what is generally accepted as triggering kinetic retaliation amongst nation states. In addition there is the potential for damage done to be reversed, a degree of plausible deniability, and an ability to amplify the effects of other traditional capabilities.

This mix of properties mean that cyber weapons lend themselves to particular forms of conflict. As Madeline Carr notes in her book on US Power and the Internet, 'Whilst a material view of power and technology may have been useful in understanding the dynamics at work in conventional conflicts and the nuclear age, IT lends itself to unconventional conflict characterised by anonymity, geographical dislocation, asymmetry, previously less significant actors on par with states and the interdependence of industrialised states in a vulnerable global network [20, p. 37].'

This chapter will describe the nature of cyber weapons, examining what makes them different from their traditional counterparts. This will be at a high level but will help inform analysis when drilling down into individual attacks.

2.2 The fifth domain of warfare

Although many actors can perform attacks in the cyber domain, the ten chosen examples are attributable to nation states or proxies acting on their behalf. As my study focusses at the higher end of cyber effects this is no surprise given that cyber technical innovation is mainly a preserve of governments and militaries or their proxies.

The US formally designated cyberspace as the fifth domain of warfare in 2011 [5], adding to the other four domains of land, sea, air and space. As these established domains became accessible the military have had to understand their nuances and the advantages and disadvantages of each have been recognised over time.

Characteristics of each of these domains are summarised in Table 5 so a comparative overview can be quickly obtained. The column for the cyber domain has been slightly modified form the original version, with modifications shown in italics and described in footnotes 1 and 2.

Conflict plays out differently in different domains determining how they are used, whether modifying machines or human behaviour, or monitoring or physically interacting. Knowledge of the nuances of each domain are essential for any grand strategy developed for it. At the 2018 Asian Black Hat Conference it was noted from historic strategies: 'If you ask a sea Admiral about war strategy he would say 'cross the T' but this would make no sense in the air where you need high manouvrability, skilled pilots, superior numbers to your opponent with an above-behind position, not a 'crossing the T' [23].

		Domains				
		Land	Sea	Air	Space	Cyber
Characteristics	Speed	Slow	Slow	Quick	Very quick	Almost instantaneous *after ground work done note 1*
	Operational reach	30% globe	70% globe	100% globe	100% globe and in space	100% globe and in space but only if IT networks
	Legal (restraint on collateral damage)	Possible to prevent	Possible to prevent	Can be difficult to prevent	Theoretically near impossible to prevent	Extremely difficult to prevent
	Domain dynamism	Can be altered with effort	Geography of operating area remains a constant			Changed at will
	Domain entry operating expense	Cheap	Relatively expensive	Significantly expensive	Extremely expensive	Very cheap *at lower end of capabilities Expensive at higher end note 2*
	Direct effort	Yes	Yes	Yes	Yes	No

Table 5: Comparison of the five domains of warfare [21, p. 22]

Note 1: Reconnaissance of the target is essential and can take months. The cyber weapon would not be successful if this groundwork were not completed so needs factoring in to timescales

Note 2: Simple tools can cost a few dollars. However, attacks requiring a high level of skills and reconnaissance such as Stuxnet can cost many millions. A single zero day vulnerability in itself can be worth over a million dollars [22]

Cyber adds additional dimensions to the conflict arena. There is not, as yet, a widely accepted understanding of strategy in the cyber domain the way in which there is within say in the maritime or air domain. Existing government attempts to define their cyber strategy do exist, however, such as the UK National Cyber Security Strategy 2016-2021 [24].

2.3 The battlefield

At a government hearing in 2000, Senator Robert Bennett showed the attendees a ‘map’ of the Internet and emphasised that there were no oceans dividing up the world. He made the point that ‘when you start talking about either national security threats or commerce in a world in which there are no oceans and no continents, you realize that we are not talking about a new tool to use in commerce or a new weapon to use in war. We are talking about a whole new place. We are talking about a whole new universe that is different from any that we have structured our Government to defend or our economy to market in the past’ [20, p. 98].

This lack of natural boarders and the effective removal of boundaries between states means strategies have to evolve with the frontline clearly demarcated no more. Five items of important will now be discussed for this new battlespace: its reach, its speed, its volatility, target dependency and the belief offense has the upper hand.

2.3.1 Reach

Three main points separate the cyber domain from the other four domains of warfare:

1. The cyber domain extends to any part of the world that is connected;
2. The same networks are used by individuals business and governments;
3. This creates the risk of collateral damage and unlike in conventional conflict, that risk is not isolated to the foreign target. For example, a cyberattack on a foreign country could affect individuals in your own country.

The reach of cyber weapons is limited only by network connectivity to carry the code to its target. This battlefield can therefore be changed at the flick of a switch, with targets disappearing instantly or reappearing again as quickly as they left. This makes it hard to compile a list of well understood targets as happens with say conventional targeting of physical buildings, infrastructure, vehicles etc.

2.3.2 Speed

The detection and impact of a cyberattack can unfold in fractions of seconds, which is an extremely short period of time compared to traditional weapons. Even hypersonic missiles take fractions of minutes to reach their target. These millisecond timescales when cyber weapons are used can strain crisis management procedures, especially in governments which operate at the speed of bureaucracy. Things move so quickly that defence can *only* be effective if it is automated, but without a human in the loop creates a range of challenges and risks [25].

The development of cyber capabilities on the other hand takes longer, with time needed to gather intelligence on a target and put together a tailored cyber weapon possibly taking weeks or months.

2.3.3 Volatility

With physical attacks it is usually possible to predict what the physical effect will be; modelling can be done on blast radiuses based on payloads of bombs for example. Exceptions may occur if a model has not taken factors into account – such as poor building design or unknown gas lines increasing the damage caused – but usually within certain tolerances modelling can reflect reality [26, p.69].

With some cyber weapons on the other hand it may be difficult or impossible to predict the weapon's effect, or to determine the impact after the event. Even Stuxnet, which was an example of a highly targeted attack, ended up on systems far from the Iranian nuclear facility. With an attacker doesn't care about specific targeting collateral damage is no barrier, as the WannaCry ransomware showed, spreading quickly across 150 different countries [15, p. 278].

The variety and novelty of cyber weapons are such that modelling to predict the exact impact, and geographic extent, of their effects is difficult. There is the potential for the

attacker to experience negative effects of their own cyber weapon – malware could spread on their own systems or cyber weapons could have cascading effects, for example on financial market instability – so called 'blowback' events. 'While customization of the payload can reduce the possibility of unintentional civilian harm, the indirect effects of a cyberattack can still be enormous if the affected computer systems support essential social and economic activities [26].'

2.3.4 Target dependence

Cyber weapons have extreme 'target dependence', meaning their effectiveness depends strongly upon the characteristics of the target, more advanced capabilities operating on a one-weapon-for-one-target basis. In such cases a team planning a cyberattack will need to tailor the weapon to the detailed specifications of the system it is targeting.

The effectiveness of a cyber weapon can be annulled with just a small change made in how a targets machine, system or network is configured. This demands that information collected in reconnaissance operation on a target 'must be precise, high-volume, high-quality, current, and available at the time of weapon's use [27, p7].'

In contrast, this is not true of weapons in the other domains of warfare, 'Any ship hit by a torpedo with a sufficiently large warhead will be damaged, whether the ship is made of wood or steel [27, p7].'

2.3.5 Offence dominance

The majority of literature discuss that within the cyber domain, the offence has the upper hand [28]. The perception that cyber is offence-dominant has led to nation states building up cyber capability in a race for dominance.

Within the physical domain, the visibility of the scale, and nature, of a nation's capabilities are clearer to see, with an order of expenditure, dominance and influence in external nations policy being apparent to all. Such determination to develop offensive dominance and the belief that mutually assured destruction was required to prevent deployment of the most powerful weapons manifested itself in the Cold War. Since the demise of the Soviet Union, the US with its' superiority in numbers and capabilities has been able to play the role of 'the world's' policeman', its' military power swaying political decisions many continents away.

Within the cyber domain, the scale of operations and funding levels can be far below manning an army, but the ability to influence and manipulate is desirable and the playing fields levelled up. Russia has used cyber and other capabilities to destabilise situations, in contrast to the idea that missile arsenals were ways of ensuring the status quo.

2.4 Under theorisation

In the introduction to his 2020 book Ben Buchanan states, ‘For military leaders, cyber capabilities may seem like tank battalions: reliable assets that can be deployed against a wide range of targets and whose force is easily understood.’ [15, p.8]. He goes on to say that these comparisons are misleading with cyber capabilities being non-intuitive and not as ’dependable, fungible, or retargetable as traditional arms’. Finding that ‘while most policymakers and scholars understand what nuclear weapons and tanks can do, the possibilities, pitfalls, and processes of hacking missions are comparatively opaque [15, p. 8], [29].’

Even though people have been writing about the implications of networked computers on national security since the 1960’s, there seems to be a knowledge gap within government and scholarship in regards to cyberspace. Attempts to apply models from the Cold War, based on ideas such as deterrence and signalling have proved unsatisfactory [30]. What could be just a minor incursion into a network for intelligence collection could be seen by the defender as a cyberattack, raising the risk of escalation. More research is needed in how deterrence works in this space [25].

This task would usually fall within the remit of international relations scholars but canonical theories such as realism would be solely state focussed. The actions of private actors would not feature in these studies given actions of a non-state actor very rarely have national security significance, which is not the case in the cyber space domain. There are now more scholars thinking about the role of private actors, however, such as feminist theorists [31] and those studying the cyber domain [3].

The focus here has been on technology and how it influences power balances between states, not on the emerged capabilities and empowerment of private players [32]. These non-state actors are eroding traditional theories of state centric analysis and shows that international relations theorists will need to include these players and not just focus on states.

2.5 Threat assessment

When a nation state completes a threat assessment on potential adversaries it would assess their perceived tactical and strategic capabilities, along with the weapons they possessed and had access to. Historically this could have been done by counting ships or tanks, assessing military factory production levels or looking at storage bases housing weapons, for example.

While states retain a lead in assessing inventories for armed forces, there are still open source analysis which can provide an assessment of the military power of nation states [33]. The count will be indicative – a country may engage in denial and deception over its military capabilities – but at least there is something to seek out and count.

With cyber weapons there are some buildings which can be examined (offices or data centres for example), satellites and ground stations that can be tracked, cable routes locations, technology companies which report partnerships with governments, catalogues and marketing material for contractors, universities offering information

security training programs, academic papers on cryptography, standards bodies, reports of supercomputer speeds, and experiments in quantum computing. These are visible things, but their usability and utility is more difficult to interpret than say vehicles and guns.

With cyber weapons there are also no signs to interpret from which predictions on intentions can be formed, such as reservists being called up or ships heading out of ports. This has made assessing cyber capabilities, actions and intent more difficult than in the other four domains. Academics have more difficulty accessing the cyber domain for research than military matters and the public know much less about cyber weapons than military matters in general.

In addition, with traditional weapons there are some bounds on advancements with a reasonable estimate of current capabilities being possible based on previous capability and experience.

This is distinct from cyber weapons which are not as bounded - each new malware potentially having completely unrelated features with the ability to achieve very different things. Indeed, the trove of capabilities stolen from the NSA by the Shadow Brokers in 2016 revealed tools which the information security community did not believe to be possible [34].

As has been noted in the book Cybersecurity and Cyberwar, 'Their [cyber weapons'] non-physical nature means that they can be produced and stored in a manner and number that makes the already tough task of threat assessment an order of magnitude more difficult [26, p. 149].' P.W. Singer and A. Friedman go onto to say, 'An enemy might surprise you with a new tank, but it wouldn't drive at 1,000 miles per hour faster than a current version [26, p. 149].'

2.6 Attribution

Attribution can be difficult in cyberspace and is achieved through long-standing observation and multiple data points rather than being quick and simple.

There are generally two types of attribution, technical and geographic sources. A nation state intelligence agency may have access to sources which support attribution and / or the geopolitical landscape could add to the evidence of attribution. In the Sony Pictures attack for example North Korea would be the main actor who would benefit geopolitically.

Cyberweapons are sometimes unattributable which means either that the defending state doesn't know who the attacking state is, they can't prove who they suspect it is, or there is plausible deniability. A lack of direct attribution through technical and geographic sources could lead to responsibility for attacks assigned in order to suit a political narrative.

It is usually the case that attribution is easier when looking at traditional weapons. There can be exception to this – for example snipers shooting rifles designed to avoid detection, the utilisation of weapons produced by enemy countries, or attackers

directly signing their malware to ensure credit for an attack - but usually traditional weapons are easier to attribute [26, p. 69]. Bruce Schneier made this point rather well commenting, ‘When you’re attacked by a missile, you can follow its trajectory back to where it was launched from. When you are attacked in cyberspace, figuring out who attacked you is much harder [35 p. 203].’

The difficulty of attribution within cyberspace means threat actors can seek to avoid consequences arising from their actions by hiding behind the anonymity given by the medium. Even if identified, the process may have taken so long as to allow the attacker to have relocated beyond jurisdictional boundaries. If threat actors believe cyberattacks can be conducted anonymously then it could cause them to become more daring in their actions – something observed in the criminal domain with fraud attempts becoming ever more brazen.

The opaqueness of the cyber domain may have benefits. The target of an attack can more plausibly deny knowing where an attack originated if it does not want to respond. This could give the benefit of being able to stand down from retaliation without damage to its reputation and resolve [36, p. 58].

2.7 Proliferation

In many cases the use of kinetic weapons results in them being destroyed along with the target. Even when weapon systems or platforms are captured intact by the adversary, this does not automatically give the adversary the capability to use that weapon. Whilst there are cases, such as the capturing of a US Sentinel drone in 2011 which was reverse engineered by Iran [37], this event is relatively rare and often the result of failures within the delivery of the weapons.

With cyber weapons the destruction of the means of delivery on impact in the majority of cases does not occur. Code rarely destroys itself when it has completed its purpose (often because the subtlety of intended outcomes does not permit this), allowing any code found on a machine to be reverse engineered [38]. This was seen when the Stuxnet code was analysed and widely published, resulting in components of the code being repurposed and used in future attacks.

With cyber weapons the reuse of a weapon is also much cheaper than for conventional weapons which usually require special chemicals, metals and manufacturing processes which are often highly regulated. A cruise missile might be retrieved in-tact for example but the adversary may not have the technical capability to replicate the technology for example. Once a cyberweapons mechanism of deployment and use have been recovered replicating these is far easier and quicker than conventional weapons [39, p.279].

The theory of non-proliferation its similar in the traditional and cyber domain in that the aim is to stop the spread of dangerous weapons. To stop proliferation in cyber the previously used of code from cyber weapons, design techniques, knowledge and information on zero days would need to be prevented [39, p. 279]. This is arguably

harder to monitor than nuclear weapons, given the more limited physical development signals within the cyber world.

The Shadow Brokers revealing NSA hacking tools is an example cyber weapon proliferation [34]. An NSA Territorial Dispute model was also released in these disclosures which could be seen as an example of the NSA's ability to track cyber capability by other states [40]. Within the US 'The Vulnerabilities Equities Process' is used to decide whether to keep or disclose vulnerabilities [39, p. 283], discussed further in Section 2.13, which can be used to adjust the US cyber arsenal.

2.8 Legal aspects

'A cyber weapon performs actions which would normally require a spy or a soldier, and which would be considered either illegal or an act of war if performed directly by a human agent of the sponsor during peacetime [41].' An act of war is typically defined as 'an aggressive act, usually employing military force, which constitutes an immediate threat peace [42].'

Within the kinetic realm there are international laws and agreements which apply. The laws of war are a set of international rules and conventions which limit the actions of the belligerent in a war or conflict. Article 5 of the NATO treaty for example provides that 'if a NATO ally is the victim of an armed attack each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take the actions it deems necessary to assist the Ally attacked [43].'

In 2013 a group of United Nations (UN) experts reached a consensus that existing international law applies in the cyber domain [44]. The US has always insisted the Law of Armed Conflict applies to cyber domain, with the US DoD Law of War Manual explicitly allows offensive operations in cyberspace for damaging or destructive purposes as long as they are conducted in accordance with the laws of war [45]. However, other states including China and Russia have queried if the Law of Armed Conflict are adequate arguing for the development of new, cyber-specific legislation.

To try and bring some international consensus to the cyber domain, the 2013 'Tallinn Manual on the International Law Applicable to Cyber Warfare' was written [46]. It is not a legally binding document but a restatement of how international law applies to the cyber domain, in particular the rights of one state to resort to war against another and international humanitarian law.

The second edition, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations', was published only four years later in 2017. In this new edition there is a scenario where a cyberattack is used to 'acquire the credentials, with the intent of threatening to conduct cyber operations against the system in a manner that will cause significant damage or death' [47]. Although, although not legally binding, it is noteworthy this was new to the second edition reflecting the level of physical destruction cyberattacks can achieve and their growing scope [48, p. 239].

Actions in the cyber realm are far too frequent, with the consequences of these actions too diverse for policymakers to come up with a case-by-case action. It has even been noted that the burden of bureaucracy to classify and respond to cyberattacks alone may cause sufficient harm to an enemy to induce attackers into action. This can be thought of as DDoS operation against civil service personnel already over-burdened with responding to unending incidents [49].

However, cyberspace does have existence in real space with basic physical components such as routers, machines, and human users. As such activities and users are partly subject to the normal controls of the territorial state: legislature, courts and police forces [3, p. 161].

2.9 Cost

As a physical item, the costs of development, maintenance and deployment of traditional weapons is both quantifiable and generally publicly available. Examples of rough costs for weapon systems and platforms used in physical attacks are approximately: munitions $0.5-$10 million, aircraft $100-$200 million, ground units $0.5-$3 million and naval units $0.5-$6 billion [50].

It can be more difficult to assess the costs of cyber weapons. According to one source, with the exception of the atomic weapons, cyber weapons cost more in research and development [26]. But simple tools within cyber can cost a few dollars, such the $25.95 off-the-shelf software used by Iraq in 2009 to capture video feeds from US drones [51], or even be free to download. However, zero-day vulnerabilities for an iPhone can cost over $2 million, as noted in Figure 3.

In addition to purchasing vulnerabilities, the cost of cyber weapons would also have to include the cost of training and paying the developers of the code. Given government pay scales are lower than the equivalent position in the private sector, attracting and retaining talent in the cyber domain is an issue.

It has been noted that cyber weapons are probably getting cheaper due to four processes [22].

1. Labour gets more efficient as attackers spend less time experimenting, leading to fewer mistakes in code.
2. Malware development gets standardised by developers in exploit tool kits, leading to an increase in efficiency.
3. Building upon and reusing existing tools and code allows more efficient cyber weapon production - even actors with limited resources can download open source tools.
4. Shared experiences of vulnerabilities, exploits and propagation techniques allows others peoples ‘lessons learned’ to be shared - this was seen with the Ethernal Blue code which was used in WannaCry and NotPetya [52].

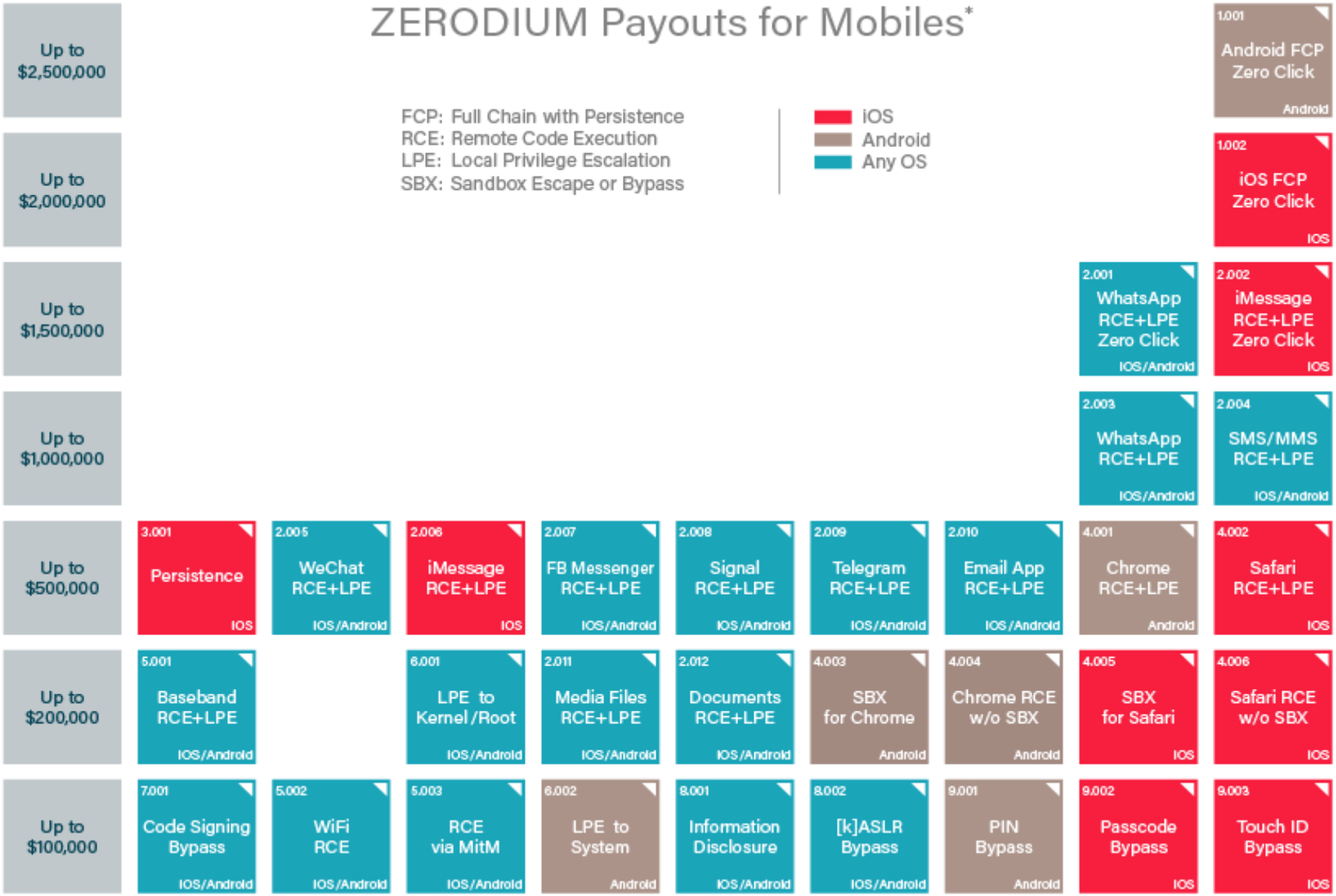

Figure 3: ZERODIM payouts for mobile phones vulnerabilities [53]

There are barriers to cost reduction though, with defensive measures becoming more common forcing an increase in attacker capability to be able to access networks. Cyber security is become increasingly noted at board level as is management knowledge of the importance of cyber security, with defences such as network segmentation, vulnerability patching, firewall implementation and secure remote access methods being increasingly used.

Finally, the malleability of the domain makes weapons only effective for a short time. With new products being released and vulnerabilities being patched, cyber weapons can become instantly useless (or working only against unpatched systems). Therefore, the development of cyber weapons must be a continuous cycle with resources and personnel being constantly available to write new code for vulnerabilities found.

The cyber weapons market is not truly open, with many actors in the field wanting to obtain vulnerabilities for illegal outcomes. This leads to underground trading and prices being hidden from view. Price dynamics of skills and vulnerabilities could differ more than wages and vulnerabilities payouts would suggest. For example a particular case could involve a one off payment for services, such as the approximately $1 million paid by the US authorities to unlock the San Bernadino attacker's iPhone in 2016 [54].

In 2006, a project was produced outlining almost 200 tasks required to produce a nuclear weapon, identifying costs and barriers to nuclear development. A similar concept for a cyber weapon may be challenging considering the rapid pace of technological change but until military strategists, policymakers and intelligence officials understand the cost drivers for cyber weapons, they will not have any basis to claim whether cyber tools are getting cheaper or who can access them [22].

2.10 Diversity of actors

The cyberattacks against Estonia and Georgia demonstrate the ease which civilians can cause harm across national borders. 'The diversity of cyber players and the possibilities for cooperation among them establish conditions for fundamental instability [25].'

Ben Buchanan even goes as far as to suppose that the biggest difference between the cyber domain and the other domains is the role of the private sector, rather than its speed or attribution difficulties [55]. He observes that governments do not have the levers in cyberspace needed to solve cyber conflicts.

In many circumstances governments seek private sector cooperation and council, such as from Microsoft, Fire Eye and Crowd Strike which have more subject matter expertise in this arena, may have better access to data from private networks and users and are more agile. Also 85% of critical infrastructure is in private hands [20, p. 99] meaning for things to get done, the private sector owners of this infrastructure are needed.

'In short, the cyber revolution's most profound disturbances may be its effects, not on the balance of power but on the balance of players [32].'

2.11 Life expectancy of weapons

The lifetimes of physical weapons are dependent on their ability to weather the elements, survive enemy fire or avoid being made obsolescent by changes in defensive technology and from newer models. Eventually all physical weapons degrade but they usually have lifetimes into decades if there is not an active war ensuing. A fighter jet for example would have a lifetime of around 30-40 years, and if there is no war can be used for military parades and shows of force.

Cyber weapons have a similar 'rusting' process like traditional weapons, in that they have a finite life, after which they will not work [56], or have limited use. For example, a zero-day exploit for the Windows Operating System will eventually be found and patched or a newer versions released, making it useless except in old, unpatched versions. The investment in cyber weapons can be millions of dollars and then suddenly they can no longer operate on the intended target, leading to the situation that they are simply written off.

A study on life expectancy of cyber weapons has been performed based upon how many were independently discovered and redisclosed by another group. It found average life expectancy of zero day exploits and their underlying vulnerabilities to be 6.9 years, with 25% of vulnerabilities not surviving to 1.5 years and 25% still active after 9.5 years [57]. This gives some indication of at what point an opponent may also have obtained your cyber weapon or patches to prevent activation.

2.12 Intrusion and attack may look the same in cyber

When defining, for the purpose of this project, what constituted a cyber weapon it was noted that infiltrating networks to gather data for intelligence purposes did not. The prevalence and existence of cyber espionage being an extension of traditional methods, which is a fact of life between nations.

Unfortunately, those techniques used to gather intelligence and those techniques used to inflict damage – which were defined as cyber weapons – are hard to distinguish in practice.

If malware is therefore detected on the network, systems administrators cannot be certain of the infiltrators intent and they may misperceive an intelligence operation as an attack. The malicious intent of an intrusion would only be known for certain when the attack has commenced, which would too late for the victim.

Interaction with the target prior to a cyberattack is often a prerequisite for success, with prior reconnaissance and planning required [27]. This could include installing a 'back door' to grant access later for downloading a customised payload or monitoring of the network to account for changes to the target's system.

Given network reconnaissance is usually done prior to an attack and also during an attack, this gives rise to uncertainty as to the intruder's intent, with nation states having

to interpret all intrusions into critical infrastructure as threatening. This could lead to retaliation before the actual attack has even begun.

2.13 Improved defences counter attacks globally

One major nuance of the cyber domain is that to maximise the impacts of your attacks you have to leave yourself at defensive parity with the enemy – with most countries using the same network protocols, operating systems and underlying hardware any exploit you discover will be present everywhere, and the corrective patches issued everywhere. There might be cases where exploiting a vulnerability requires sufficient computing resources that in practice not everyone can access it but in general, fixing a vulnerability fixes it for everyone and leaving a vulnerability keeps everyone exposed to it. Countries seeking to use an exploit against an enemy therefore leave themselves open to the same exploit being used against them.

With increased defences negating attacking capabilities, the US government use 'The Vulnerabilities Equities Process' to determine if software vulnerabilities should be disclosed or not [39, p. 283]. If vulnerabilities are retained by the government they would go to their cyber arsenal for use if required in a cyberattack. Disclosures are usually released to the vendors of the software to patch and passed on to the public. These patches close the vulnerability, preventing the weapon being used against the vendors systems worldwide.

It seems like an impossible puzzle, with no way to simultaneously defend networks whilst leaving foreign networks open to attack given many people use the same software [58, p. 250]. The US not patching systems runs the risk that if another country has found the same vulnerability that could be used in a cyber weapon against US systems. Patching all vulnerabilities means the US would have fewer cyber weapons of its own if they were needed.

There are supporters and detractors of both ideas, with the process reportedly tilted toward disclosing vulnerabilities under the Obama administration [27, p. 4]. However, this could be swayed toward stockpiling or even more towards disclosure depending on the government of the day and the geopolitical environment that they find themselves in.

This dilemma is a concept which wouldn't raise its head within the physical domains, adding to the different ways of thinking required when trying to grapple with the cyber realm.

2.14 Conclusion

In Bytes, Bombs and Spies the author's note, 'More clearly delineating what's new and what isn't in offensive cyber operations is an important step forward [27].'

The information presented in this section represents the main factors which are different in cyber weapons compared to their traditional counterparts. Even creating a map of the cyber domain is challenging, with the landscape constantly changing as devices are connected and removed from the Internet.

Analysis will now be completed using strategic frameworks covered in Section 1. Within Section 3 the important nuances of the ten cyberattacks will be described and then analysed using the PESTLE framework, along with two comparable physical attacks. In Section 4 the Porter's Five Forces framework will then be applied to the case studies to investigate the market dynamics of this arena.

3. PESTLE analysis of cyber and conventional weapons

3.1 Introduction to attacks

Ten attacks have been chosen in order to complete a comparative analysis. The attacks chosen cover a period of ten years and include political and financial motivations affecting both companies and nation states. The rationale for this selection is to obtain as wide a range as possible in terms of skills used, impact caused, sectors affected and geographic spread.

The focus will be on the effects the attack was trying to achieve (as well as the realised effects, if they were they). The cyberattacks will be compared with traditional ways of achieving an effect comparable to that achieved through the described cyber means. Two traditional alternatives will be assessed, one being a low impact example with the other a higher impact example. The ten attacks covered are shown in the timeline in Figure 4 and will be completed in chronological order.

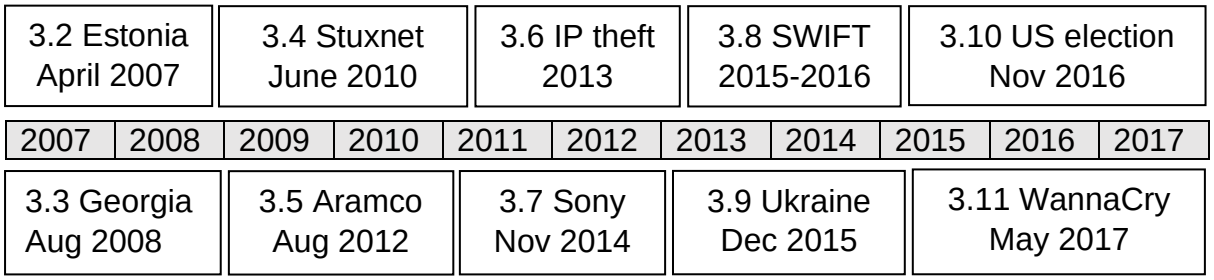

Figure 4: The ten attacks considered mapped to section numbers

For the PESTLE framework in each of the six categories the three alternative ways of achieving the same effects – cyber, low level and high level intensity alternatives – will be ranked based on which achieved the best and worst outcomes for the aggressor. This will give a numerical way to compare attacks.

- Final scores are an indicative measure of the greatest **return on effort for the attacker, for the cost incurred**. A higher score indicates the superior choice

These scores represent a qualitative assessment based on my own judgement and interpretation of the attacks, rather than a scientific analysis. My prior experiences working within the PwC Advisory practice provides me with the skills and knowledge required to apply business strategy frameworks to an area which is traditionally analysed more broadly through the lens of nuclear or military strategy.

To determine the overall score for each method values will initially be assigned. These will be 2 for best, 1 for medium and zero for the worst outcomes in each of the six categories.

The six categories of PESTLE will themselves be weighted as the relative importance of political success (or failure) will, in general be higher than the environmental impact in the eyes of the attacker. Political, Economic, Societal and Legal will have a default weight of 3, Technology 2 and Environmental 1.

This method allows the relative importance of each category to be taken into account, and whilst we will hold these constant in the majority of the attack, each of the ten examples chosen will be reviewed at an individual basis to adjust levels if needed. The 2016 election interference for example will have a very high political rating for example so the scoring on the 'P' of the PESTLE will be adjusted to reflect this.

The full PESTLE frameworks for each of the ten attacks are to be found in the appendices with only a summary of the scoring from the PESTLE presented here.

3.2 Estonia – April 2007

Estonia has a population of 1.3 million people and has a relatively high degree of online integration in day-to-day life – elections are held online, 40% of its people read a newspaper online daily and over 90% of retail bank transactions are performed over the Internet [59].

A cyberattack lasting two weeks through April and May 2007 showed the ability of cyber technologies to disrupt the economic affairs of this nation.

The event sparking this attack came on 27 April 2007 with the removal of a statue in the country's capital, Tallinn. To Russia the statue commemorated the Soviet dead in World War II, but to the Estonians it symbolised oppressive occupation after they suffered mass deportation of their people to Siberia by the Soviet secret police. After 16 years of independence, Estonia ignored Russian government protests and warnings that removal would be 'disastrous for Estonians' [59].

The resulting cyberattacks unfolded on multiple fronts. Script kiddies, stoked by nationalism on Russian-language chat rooms, were given simple executables on hacker websites to download and unleash. These, relatively unsophisticated, ping attacks repeat simple requests to web servers hundreds of times a second and, in numbers, can overwhelm a server. Botnets made up of hundreds of thousands of hijacked computers were made to repeatedly flood designated Internet addresses with useless network-clogging data, a DDoS attack. Such attacks overloaded target server's processors and hogged bandwidth. Finally, the more sophisticated hackers infiltrated individual web sites deleting legitimate content and posting their own messages.

Whilst many companies suffered the principle targets of the attack were the essential electronic infrastructure of Estonia – government communications, major commercial banks, telecommunications, name servers (the phone book of the internet), ATM machines in Tallinn, newspaper websites, and other media outlets were all taken down.

To highlight the scale of the attack, on May 8th, at exactly 11pm, Estonia was hit with traffic at 4 million packets per second, a 200-fold increase in usual traffic levels [59]. Nearly 1 million computers globally – equivalent to the entire Estonian population – suddenly navigated to Estonian sites squeezing the entire country's bandwidth 59capacity. Given attackers were changing malicious server requests to evade filters it was noted that the perpetrators were sophisticated.

The majority of the Estonian population were affected through this attack. Although physically the attacks were not destructive they inflicted considerable harm on the

political, economic, and social world causing national disruption of government and financial activities. This has been noted as the first known cyberattack on an entire nation [60].

Three days after the statues removal from a prominent place in Tallinn, it was installed in a military cemetery in the suburbs. The Estonia government stated that it was always its intention to relocate rather than remove the statue entirely.

Although Russia denies that they were behind this attack, they are attributed by most countries as having been the perpetrators [61]. But within the cyber domain Russia are still able to hide behind a veil of 'plausible deniability'.

A member of the Estonian parliament hypothesises the attack could even have been a test on a NATO member state, 'Attacking us is one way of checking NATO's defences. They could examine the alliance's readiness under the cover of the statue protest' [59]. Estonia wanted NATO to declare that its sovereignty was violated and thus trigger the self-defence part of the NATO treaty, Article 5. However, the attack had been in the cyber domain not the physical, and Allies did not want to be in a major crisis with Moscow, so no response was given from NATO.

After the attack Estonia realised how vulnerable the country was given its highly connected society and it acted to ensure nothing similar could ever happen again. Estonia has set up a cyber defence league, a more formal and transparent body than patriot hackers, more akin to a cyber militia – an organised group of non-professionals which are willing and able to use cyber for political goals. Recruitment to this group was helped by the effects felt by the Estonian population in the cyberattacks.

It was also clear to other countries that they too were vulnerable to cyberattack, with state powers putting cyber concerns further up the agenda. It showed aggressive states could temporarily cripple a rival's infrastructure whilst at the same time maintaining plausible deniability.

As a direct result of the Estonian attacks, the 'Tallinn Manual on the 'International Law Applicable to Cyber Warfare' was also developed [46], [47]. This outlined international laws considered applicable to the cyber realm aiming to establish a global norm.

<u>Comparative examples:</u>

The comparison of traditional means with cyber weapons will focus upon ways in which another country can impart political force in order to incite civil unrest and mass panic so as to influence and change political decisions by governments. Specifically these will be: (1) propaganda and inciting street protests; and (2) a kinetic military show of force. Both of these were actually found in this example along with the cyberattack, but they will all be treated in isolation for this analysis.

(1) Before the statue was taken down there were riots and protesting in the streets of Tallinn by mainly Russian residents, with shop fronts being smashed, cars being flipped over and rocks being thrown at riot police [59]. Propaganda campaigns were used to organise protests and script kiddies with Russian national patriotic fever being stoked up and fake news being spread – mainly about the war statues removal.

(2) On May 8th in Moscow's Red Square 7,000 Russian soldiers marched past the President to celebrate Russia's victory over Nazi Germany, at the same time as the cyberattack. As fighter jets flew through the skies, Putin's speech contained a thinly veiled reference to Estonia. He said, 'Those who are trying today to... desecrate memorials to war heroes are insulting their own people, sowing discord and new distrust between states and people.' [59]. Although this military parade was planned for this time long in advance, the PESTLE will be rated on an show of force not within a planned calendar event.

Results from the Estonia attack are summarised in Table 6 with the full PESTLE analysis in Appendix 1, Table 18. Scores show the best return of effort for the attacker is through either completing the cyber or the propaganda action. Cyber scored highly in the political and socio/cultural categories with propaganda scoring highly in the economic and technical categories.

	P	E	S	T	L	E	Total
Cyber	8	0	8	0	2	1	19
Propaganda	4	6	4	4	0	1	19
Military force	0	3	0	2	4	0	9

Table 6: Summary PESTLE analysis for Estonia

3.3 Invasion of Georgia – August 2008

It is likely Russia coordinated a cyberattack during its invasion of Georgia in 2008 to augment invasion forces. This was achieved through targeting communication channels so as to blackout or severely limit information transfer within the Georgian defence forces. This not only hindered reaction and responses by the military and parliament but also enabled Russia to control reporting of the situation on the international stage. By preventing Georgian communication with the outside world, especially over terrestrial media and internet channels, Russia controlled the narrative of the war.

The attack was noted for being direct and well organised, even at the initial stages, to accompany the process of invasion. The preliminary work came a few weeks earlier in July, with a DDoS attack on the President of Georgia's official website. This, along with Russian actors constantly scanning Georgian communication networks, could be seen as a rehearsal for the larger attack in August [62].

The main cyberattack commenced soon after Russian forces invaded with conventional forces. Websites of the President, Governor, Ministry of Foreign Affairs, Parliament and news websites of Georgia were taken down. When the President's website was recovered it suffered a defacement attack. The largest commercial bank in the country was also attacked, as were websites of other countries covering the conflict not completely in Russia's favour, such as within Azerbaijan [63].

Compared to Estonia, Georgia was not as highly dependent on IT, with internet usage of the populations 57% and 7% respectively [63]. This meant the effect on the population and the state was not as great as for the Estonia attack in 2007. However, partial take down of information channels simplified the implementation of military

tasks for Russian armed forces, creating an information vacuum for Georgia and superiority for Russia.

Even after more than a decade of subsequent investigation, there is a lack of definitive proof linking this attack to the Russian Government even though Georgia believe Russia was behind the cyberattack. The inability to assign responsibility highlights an advantage of using a cyber militia (Russian patriotic hackers) for deniable operations. The campaign wasn't covert but involved activity which had enough ambiguity that it could be denied by Russia, despite it being the only obvious beneficiary.

Actions which constitute an 'act of war' are defined as aggressive acts of one nation against another, which are usually measured in terms of loss of human life and/or levels of physical destruction. Just focussing on the cyber part of this attack would not meet these criteria for an act of war.

Comparative examples:

The comparison of traditional means will be ways in which another country can cause communication lines – internally and externally – to be affected. These will be: (1) physically cut communications channels through internal sabotage; and (2) through more physical military forces attacking communication networks.

(1) Requires a dedicated covert team operating within the country and like the cyberattack will need planning a long time before the operation is executed. Multiple teams will need to coordinate activities to create mid-term disruption to multiple communication channels (internet, TV channels, radio) in order that news out of the country is disrupted to the extent of the cyberattack. In reality, maintaining such blackouts and / or control for a significant period of time through such sabotage would be difficult to ensure and maintain, with multiple single points of failure. Cyber allows attacks to scale with the network, in a way that physical disruption might not.

(2) Military operations were already in effect whilst the cyberattack was underway. This option would increase these operations in order to take out the communication channels across the internet and TV channels by bombing satellite base stations and communication hubs.

Results from the Georgia attack are summarised in Table 7 with the full PESTLE analysis in Appendix 2, Table 19. Scores give the best return of effort for the attacker through completing the cyber action. Cyber obtained the highest marks in all categories but for socio/cultural and technological.

	P	E	S	T	L	E	Total
Cyber	8	6	4	0	6	2	26
Cut comms	4	3	8	4	3	1	23
Military force	0	0	0	2	0	0	2

Table 7: Summary PESTLE analysis for Georgia

3.4 Stuxnet – June 2010

In June 2010 Iran's Natanz nuclear facility enrichment program hit a major problem. Whilst the ongoing talks with the US over Iran's nuclear programme were stalling, the centrifuges required to enrich uranium were malfunctioning and breaking suddenly, despite the controllers showing no signs of problems. Unbeknown to the scientists running the plant they were the victims of what is now one of the most famous cyberattacks to date.

The cyberattack is widely understood to have been a joint operation between the US and Israel, although neither has formally admitted responsibility. With the attack having Iranian scientists doubting their abilities and systems being taken off-line for inspection, the US had more time to negotiate a peace deal and, according to Kim Zetter, could possibly have prevented a military attack [64, p369].

The attack was very specific to the target, requiring detailed knowledge on the configuration of centrifuges at the facility [49]. This implies significant reconnaissance and preparation including a need to break into the facility networks ahead of time as well as a means of accessing plant designs and specifications. It was even reported that a replica of the Iranian facility was built to see if the cyber weapon would indeed work [49], and presumably stay under the radar of cybersecurity teams.

Success, in both the worm working to break the centrifuges and preventing spread and disruption to other countries, was highly dependent on information gathered from the target. The restraint shown in the design of the attack payload suggests that stealth was priority in the attack.

Far from being a simple exploit, the Stuxnet code indicated a step-up in sophistication from previous cyberattacks [64]. It relied on stolen signing certificates, suggesting attackers had access to significant resources and placed high priority on operational security [15, p. 140]. It was large in size – about 50 times larger than usual malware [64] – and utilised a large number of zero-day vulnerabilities; all factors suggesting state involvement and planning. Indeed, the level of sophistication of the attack has been cited as a watershed moment in cyber capabilities, akin to that seen with the change in weapons landscape after the dropping of the atomic bombs in World War II [19].

Stuxnet also showed the potential importance of non-state actors in cyber operations, with discovery not by Iran or another nation state but by a worker at a small security company in Belarus, Sergey Ulasen [65]. Another individual, German security consultant Ralph Langer, is recognised for his forensic work analysing the malware [64]. Langer states that the attack was, 'as good as using explosives' against the facility. In fact, it was better as the victim had 'no clue of being under a cyberattack [26, p. 117].'

For all of the sophistication Stuxnet brought to the cyber arena, the necessary defences - relying of default passwords, not patching known vulnerabilities - were both easily accessible and low-cost. Once the attack was discovered, Iran even received free expertise and patches from the global commercial and open-source cybersecurity community [66].

In stark contrast, the cost to develop and deliver the attack was high – even by conventional weapons costs – the US Bush administration reportedly authorized $300 million for 'joint covert projects' aimed at Iran's nuclear program [66, p. 27]. This amount, however, does not include infrastructure, expertise and experience already paid for in other government agencies.

From the analysis it can be seen that Stuxnet could deliver strategic results equivalent to a military strike (delaying the ability for Iran to obtain nuclear capability) whilst avoiding a high level of retaliation or even Iran finding out it was under attack for many months. The reduced destructive scale, compared to a missile strike, or a special forces raid was its appeal and strength.

Although the Stuxnet worm was successful in its objectives of delaying Iran's enrichment program it only delayed, not prevented. Also, as a result of the attack Iran's leadership realised how important cyber operations are to security and hastily tried to catch up with the West in cyber operations – a negative secondary effect.

A further downside of the cyberattack was that once the Stuxnet code was analysed it became available in open sources and was used in subsequent attacks [38]. This put into civilian hands government capabilities to anyone who downloaded it, allowing hackers to learn from, and use, the code in their own malicious attacks.

As Iain Lobban, former Director of GCHQ, states 'What was considered a sophisticated cyberattack only a year ago might now be incorporated into a downloadable and easy to deploy Internet application, requiring little or no expertise to use' [67].

<u>Comparative examples:</u>

The main aim of the attack was to delay the enrichment of Uranium by Iran in order to give time for peace talks to come to an agreement on limiting the extent to which Iran would perform nuclear enrichment.

Alternative ways to achieve this are: (1) sending in a special operations team to break into and compromise the facility and; (2) ordering a missile strike on the facility.

(1) Using a special operations team would have required similar levels of pre-planning regarding the layout of the facility and knowledge of the centrifuges as the cyberattack, but with the additional challenges of understanding the security detail, access points and infiltration / extraction routes.
The location of the facility and security surrounding it would increase the risk that this would not be successful and the team be captured. Iran was also alert to these traditional types of sabotage so success could not be guaranteed.

(2) With talks progressing as to the extent of allowed enrichment, a physical strike would have been provocative, potentially leading to a spiralling conflict.
It would have required multiple strikes and heavy duty ordnance (bunker busters) to take out given the facility was located in an underground facility. The use of explosives would have crated significant risks of radioactive material being leaked from the facility on impact and the death of personnel in the facility.

Results from the Stuxnet attack are summarised in Table 8 with the full PESTLE analysis in Appendix 3, Table 20. Scores give the best return of effort for the attacker through completing the cyber action. Cyber obtained the highest marks in all categories but for economic and technological.

	P	E	S	T	L	E	Total
Cyber	8	0	6	0	6	4	24
Special ops.	0	6	0	3	3	2	14
Missile strike	4	3	3	6	0	0	16

Table 8: Summary PESTLE analysis for Stuxnet

3.5 Saudi Aramco – August 2012

This attack disrupted operations of the largest oil and gas company in the world, which provides 10% of global oil output, c.9.5 million barrels a day [15, p. 149]. Although the attackers have never been identified some have speculated Iran may be responsible in response for an earlier attack on their energy sector [68]. This earlier attack in mid-2012 was nearly identical to the one on Saudi Aramco with speculation of Israel being the aggressor [69]. The perpetrator of these attacks are very much speculative with no attribution made by nation state, although hacking group 'Cutting Sword of Justice' claimed responsibility for Saudi Aramco [69].

As with most cyberattacks, the foundations were laid months before the actual attack, when a member of Aramco's IT team opened a malicious link in a phishing email. The actual attack was timed for Ramadan, an Islamic holy month when most Aramco employees were on holiday [70].

When it hit on the morning of 15 August 2012 the worm, named Shamoon, configured itself to run whenever a targeted computer started up, wiping files and shutting down computers. In a matter of hours, 35,000 computers at Saudi Aramco were partially wiped or totally destroyed, this number comprised the near totality of company computers [68].

Aramco technicians ripped cables out of servers at data centres globally to stem the spread, physically unplugging all offices from the Internet. Without this connection corporate email was gone and office phones were dead. Instead typewriters were used to write reports, paper used to manage supplies and shipping, and contracts passed around interoffice mail or faxed page by page [69].

In this particular attack the separation of office networks from the production networks stopped it impacting oil drilling and pumping which remained steady throughout attack. However, even without the production impacted supply issues were still present. With no way to accept payment oil sales were stopped to domestic gas tank trucks for 17 days. After this time Aramco gave it away for free to keep oil supplies flowing within Saudi Arabi [71].

To deal with damaged computer equipment the company flew employees to factories in Asia to purchase all computer hard drives on the manufacturing line. By outbidding others, Aramco bought 50,000 hard drives, leading to global shortages [71].

Even after procuring equipment it took months to get servers back up and running. There were huge losses of internal data with day-to-day operations, such as scheduling, financial records and contracts affected. The attack cost many millions of dollars to put right with all computers and servers affected being replaced, an attack which could have easily bankrupted a smaller organisation [49].

This attack bought cyber operations into view and out of espionage and covert sabotage. It was a big wake up call for businesses, showing every modern company at some level was at risk of cyberattack given the reliance on technology, even without being an IT or online business.

Its effects were even felt amongst the global population, as a security advisor to Aramco after the attack noted, 'Everyone who bought a computer or hard drive from September 2012 to January 2013 had to pay a slightly higher price for their hard drive.' [71] as well as waiting longer for it.

Comparative examples:

The attack disrupted the oil sector, affecting office and production networks. This caused a knock on effect to oil supplies through payments not being able to be processed. Thus for comparable examples oil supply disruption will be considered, namely: (1) by targeting the refineries; (2) by targeting the pipes and/or ports.

(1) Refineries are where crude oil is fractionated into its component parts, such as kerosene, petrol, bitumen and other petrochemicals – there is limited use for the unrefined base product. With a limited amount of global storage if the refineries are affected this would create disruption not only in supplying products but all the way up the value chain, pushing down prices for futures contracts and requiring a reduction in production itself. To disrupt refineries teams of people would need to be deployed in order to sabotage operations of enough of these to be impactful.

(2) Oil is transported within pipes from major oil fields to local consumers or put onto huge floating tankers to be shipped around the world. Given the size of tankers there are a limited number of ports large enough for these to dock. Preventing the unloading of oil for prolonged periods would affect not only supplies to consumers but also the ability to store supplies being pumped (well needing long lead times to reduce capacity). Disrupting oil pipe flow would similarly affect transportation and supply. This effects could be achieved through sabotaging pipes or ports.

Results from the Saudi Aramco attack are summarised in Table 9 with the full PESTLE analysis in Appendix 4, Table 21. Scores give the best return of effort for the attacker through completing the cyber action. Cyber obtained the highest marks in all categories but for technological.

	P	E	S	T	L	E	Total
Cyber	6	8	6	0	6	4	30
Target refineries	3	4	3	4	3	2	19
Target pipelines	0	0	0	2	0	0	2

Table 9: Summary PESTLE analysis for Saudi Aramco

3.6 F-35 IP theft – 2013

According to a 2017 US report, Chinese theft of American Intellectual Property (IP) currently costs between $225 billion and $600 billion annually [72]. A study by Verizon found 96% of state-affiliated attacks targeting IP in 2012 are from Chinese hackers. This cyber espionage has even been said to cause more problems than political secret theft with the New York Times describing IP theft as the number one problem the US has with China's rise [26, p. 94].

These cyber thefts include valuable trade secrets and knowledge of technology required by companies to continue making future profits. The then Director of the NSA has called IP theft 'the greatest transfer of wealth in history [73].' Economic prosperity pays for militaries, diplomacy and development efforts allowing global influence. It was noted by President Barack Obama in 2012 that IP theft undermines economic and military power [20, p97].

Commercially, theft diminishes profits and reduces the economic base. Loss of the exclusive benefits of military and scientific developments means monies invested in these by the state is obtained by others at little cost. With the original companies seeing a lower return on the capital invested in such developments, this both impacts US competitiveness as well as the willingness to continue to invest in new technology, further stifling differential innovation.

To try and address foreign barriers to US exports, Section 301 of the Trade Act of 1974 is used [74]. This allows the President to impose trade sanctions against countries which fail to adequately protect IP rights. Trade sanctions, however, are a very blunt tool and less effective in dealing with actions by individual companies.

Individuals are better dealt with through the criminal or civil law enforcement, with US IP owners having had success enforcing rights in Chinese courts [75]. The Economic Espionage Act of 1996 also aids federal criminal sanctions for the civil liability for trade secret theft [75].

James Lewis, researcher at the Centre for Strategic and International Studies, notes: 'If Chinese or Russian spies had backed a truck up to the State Department, smashed the glass doors, tied up the guards and spent the night carting off filing cabinets, it would constitute an act of war. But when it happens in cyberspace, we barely notice [3, p. 77].'

Although these cases seem to be more aligned with espionage, rather than the use of a cyber weapon, it is being considering here due to the nature of the information theft, namely design secrets for the F-35 fighter, the most advanced fighter aircraft in history. These designs included the secrets of its stealth radar and engine and were taken from the computers of the US government and private defence contractors [3].

A 2014 US-China Congressional report cites a Defence Science Board finding that Chinese cyberattacks resulted in the theft of the F-35 design [76]. The F-35 design had taken the US two decades in research and development and allowed China to replicate the technology and make a rival plane, the J-31, at a significantly lower cost [77].

The scale of this remote, nonviolent data capture gave effect greater than achieved through violent seizure by armies [3, p. 76]. Given the scale, the significance and the effect of being able to weaponize the IP, this cyberattack has here been considered a cyber weapon.

Comparative examples:

Focus on the F-35 fighter will allow comparison of a single incident, which is more useful than many issues over a longer time period. Comparative examples specifically analysed are: (1) Industrial espionage and; (2) physically breaking into offices.

(1) Industrial espionage would involve having to place someone from the Chinese state within the office of a military contractor and of the appropriate security clearance levels. This would be both a time-consuming operation as well as having a level of operational risk – the asset would need to be placed in situ potentially years before the activity occurred so as to progress to the appropriate level in the firm – although this is common in espionage.
Alternatively, an existing member of staff who had sufficient clearances would need to provide these documents. Again this would be a long-term operation; identifying the individual and finding leverage enough to get them to break the law and risk committing a federal crime. There would also be an inherent risk of false documents being provided so as to double cross the operation.
Although in practice, human intelligence operations described here would be integrated with cyber techniques for the purpose of this analysis they will be treated separately.

(2) This alternative would involve a breaking into the offices and taking out information akin to what was described by James Lewis earlier, by backing a truck up to the office, smashing the doors and, whilst not literally taking out filing cabinets, removing the digital documentation required. This would in itself require some cyber capabilities to gain access to encrypted systems.

Results from the F-35 IP theft attack are summarised in Table 10 with the full PESTLE analysis in Appendix 5, Table 22. Scores give the best return of effort for the attacker through completing the cyber action. Cyber obtained the highest marks in all categories but for socio/cultural and technological.

	P	E	S	T	L	E	Total
Cyber	8	8	0	2	6	2	26
Espionage	4	4	3	4	3	2	20
Physical attack	0	0	6	0	0	1	7

Table 10: Summary PESTLE analysis for F-35 IP theft

3.7 Sony Pictures – November 2014

The Interview was a film comedy distributed by Sony Pictures in which the North Korean leader Kim Jong-Un was depicted in a negative manner and eventually killed. North Korea perceived this as an insult, an act of ‘terrorism’ and a ‘war action’ coming not from an independent film company but from the White House itself. North Korea tried to force Sony to pull the film saying there would be ’strong and merciless countermeasures’ if it did not do so [15, p. 169], [78].

North Korea felt it imperative to stop the release of the Interview, with Kim Jong-Un’s power dependent on a deity-like image which was undermined by the film. The stakes to North Korea in relation to its release were high, but to Sony the movie was just another release among many and no blockbuster. When the initial threats to force Sony to pull the release did not work, North Korea turned to coercion through cyber means to raise the stakes.

The attack on Sony Pictures, believed to be by North Korea, began two months after their network had been infiltrated. 70% of computing power was lost by the studios and unreleased movies were leaked online for anyone to download. Employee emails, pay, social security numbers, legal issues and screenplays for upcoming movies were also released. In addition the personal views of the co-chair of Sony Pictures, Amy Pascal, on behaviour of actors, producers and others were open for all to see in a huge PR disaster [15, p. 168-184].

This attack is a change from other attacks noted so far in terms of the biggest impact to the business not being from the damage to infrastructure, but rather seeking to embarrass, damage the reputations of those responsible for the release and impact revenues from future releases. Whilst the infrastructure impact was costly in terms of down-time, replacement parts and business disruption, the severest and longer-lasting blow was from the stories from the data dumps.

Three things from the data releases stand out as being most impactful. Firstly, there were financial losses from the release online of upcoming movies, with the movie business relying on people paying to view. Secondly, personal email releases were designed to harm the future pipeline of the studios, given the business relies on good relations with high earning stars and producers. Finally, the release of wages across the business laid bare the extent of the gender pay gap at Sony, a topic very much in the headlines at the time in the US.

Sony Pictures, being a private company, had very little capability to do anything to stop these cyberattacks but to defend against them the best it could. Indeed, even which country should or could act to help the company was ambiguous given it is both an American and Japanese owned corporation.

The move by North Korea was seen as an attack on Western democracy and free speech by the US [15]. However, no matter how important these are, the US was blatantly not going to get itself involved in a war over a film.

President Obama criticised North Korea, pledging a ‘proportional response’. This was later enacted as economic sanctions, mentioning human rights violation in addition to

the Sony attack for their imposition [79], maybe to give the US room for attribution uncertainty given North Korea were denying responsibility for the cyberattack.

In this case a cyberattack was met with economic sanctions, clearly demonstrating governments not responding openly in the manner in which they were provoked, i.e. by cyber means. This could be argued as being proportional to the damage done – being mainly economic damage to a US company. As article in the Washington Post stated the US took action never done before in 'response to a cyberattack by another nation; it names the government responsible and punished it [80].'

The attempt by North Korea to thwart the film release ultimately boosted its success. Indeed, the move backfired spectacularly arousing nationalistic sentiment in the US population with the movie standing for freedom and democracy. Cinema screenings sold out and within a month The Interview became the best-selling online release ever, making $40 million on Netflix [15, p. 184].

However, even though it failed with this particular film the incident did have repercussions elsewhere. Within the UK for example BBC 4 were aiming to make a ten part drama based the plot on North Korea kidnapping a British scientist to force him to complete their dreams of uranium enrichment. After the Sony Pictures hack this failed to get funding required from investors and production was dropped [49].

Even though North Korea was the country most likely to have committed the attack due to the overtones of the films content, there was still a measure of deniability with the hacker group 'Guardians of Peace' claiming responsibility [81]. The US allege this group is sponsored by the North Korean government, which is denied by North Korea [49].

US Senator John McCain called the Sony pictures attack an act of war, stating 'When you destroy economies, when you are to impose able censorship on the world...it's more than vandalism. It's a new form of warfare [82].' In contrast to this President Obama stated that the hack was a serious matter for national security, and therefore necessitated a policy response but did not meet the criteria of war, being more an act of cyber-vandalism [82]. These two views from within the US emphasise the grey area in which this attack fell.

<u>Comparative examples:</u>

The ultimate aim of the attack was to prevent the movie release. Comparative examples used to reflect this will therefore be: (1) breaking into Sony offices to obtain compromising information and digital copies of upcoming releases and; (2) threatening to bomb cinemas and Sony offices.

(1) Information obtained through the cyberattack could also have been obtained through breaking into Sony offices. This would permit the leaking of similar material but the initial means of obtaining the data would have changed.
To achieve this would have required bypassing physical security as well as possible cryptography on machines – essentially organising a break in at the offices and hoping that information could be extracted on the night. With limited

timescales (2-3 months) to achieve exfiltration planting or recruiting an insider to access the material would not be a viable option.

During the cyberattack there was, in addition, threats made to bomb cinemas which released the movie. Although the threats were not carried out this did result in a much reduced screening of the movie to very few outlets. This will be analysed separately to the cyberattack, and has not been treated within the cyberattack analysis as a combined operation.

Results from the Sony Pictures attack are summarised in Table 11 with the full PESTLE analysis in Appendix 6, Table 23. Scores give the best return of effort for the attacker through completing the cyber action. Cyber obtained the highest marks in all categories but for technological.

	P	E	S	T	L	E	Total
Cyberattack	8	6	8	0	4	2	28
Break into offices	4	3	0	2	2	2	13
Bomb cinema threat	0	0	4	4	0	2	10

Table 11: Summary PESTLE analysis for Sony Pictures

3.8 Financial transactions, SWIFT – 2014-2015

There are a wealth of examples of nations attempting to undermine the economy of an opponent. The financial industry, within the US in particular, is a symbol of geopolitical might and a projection of power. Security breaches could threaten to undermine consumer confidence in these system and spread panic.

One case of financial institutions being targeted was the Society for Worldwide Interbank Financial SWIFT interbank monetary exchange system in 20014 – 2015. Security specialist FireEye reported the attack involved malware very similar to the Sony hack, attributing it to a group linked to North Korea [83]. The UN estimating the attackers exfiltrated $2 billion, which works out at over 7% of North Korea's gross domestic product, and impacted around 12 banks [84].

Reconnaissance in this attack was very time consuming with the need to piece together how the SWIFT system worked and gather credentials needed for authentication. As such, attackers were present in the network for many months doing investigative and preparatory work – with banks failing to detect them during this time [83]. Afterwards banks, such as the Bank of Bangladesh, were found to have had poor cybersecurity practices with a lack of security software and cheap equipment making hacking easier [85].

Once the attackers had access into the SWIFT accounts they had the power to set up transactions like any other authorised user. At this stage further malicious code was used to avoid detection, bypassing the internal anti-fraud checks in the SWIFT software. Transaction logs were also altered obfuscating where money was being sent and casting doubt on the logs depended on by the financial system – which could undermine credibility of the financial system [15, p. 273].

The printers used to make hard copy back-ups of transactions in the SWIFT system were side-lined with additional malicious code [15, p273]. This bought time for the attackers to avoid detection whilst transfer requests were being processed.

According to Ben Buchanan the attack showed an increase sophistication by North Korea hackers with toolkits used which would have been beyond their capabilities a few years before [15, p. 284]. The attackers were able to keep ahead of security upgrades not only of SWIFT but also the banks who were constantly rolling these out. It has been noted that the attackers were persistent and seems uninhibited by fear of appearances and blowback onto them [15, p. 287].

The US stated that funds were being used to fund illicit weapons and missile programmes, possibly devastating secondary effects of this attack. If North Korea was indeed behind the attack, as has been attributed by FireEye [83], then it would be the first known incident of a state actor using cyber means to steal money.

In response the US and UN announced to continue their sanctions against North Korea and to improve the cybersecurity of the financial networks [49]. A few years after the attacks, in 2018, the US Department of Justice filed criminal charges against a North Korean national who it alleged belonged to the group behind these attack [49]. These charges represent the increasing stepping up of the US pursing cyber actions through the legal system.

This was not the first time that attacks had been launched on the financial systems. In a separate incident in 2012 Iran was blamed for a DDoS attack on Bank of America, the NY stock exchange and Chase Bank [86]. The objectives did not have a monetary aspect, as in the case of North Korea attacking SWIFT, but instead aimed to disrupt transactions for customers online and to cause as much chaos as possible. Costs to banks ran into tens of millions [15, p154]. but no response was made by the US given a certain threshold of aggression had not been met and with Iran having at least some level of plausibly deniability.

Another event in July 2015 resulted in the trading of $28 trillion worth of equities being halted on the New York Stock Exchange for 4 hours [87]. This was not an attack like the cases discussed but the discovery of a coding error, revealing the potential fragility within underlying technology relied on by financial infrastructures.

A major, international, disruption of financial institutions could cause economic reverberations which would undermine consumer confidence in global markets. These psychological impacts – that of trust in the markets and that monies held were safe – would be far more damaging than the initial attack.

However, with the interconnectedness of both computer and financial systems there is also the indirect consequence of blowback, where the attacker themselves are disrupted.

The consequences of this situation is so severe that President Obama argued the US should pledge never to attack or interfere with financial markets, given the tremendous negative impact it could have in the global economic system [88].

Comparative examples:

The attacks discussed have impacts financial institutions, traditional ways this could be achieved are: (1) insider trading; (2) economic acts

(1) Insider trading is where you use privileged knowledge of trading activity (mergers and acquisitions for example) to make money out of the stock market. This would be hard to achieve across multiple companies to cause shockwaves through the system but could be a source of revenue as the SWIFT attacks were.

(2) Imposition of sanctions, issuing trading bans, escalating tariff on goods, dumping currency in large amounts and/or counterfeiting money to cause inflation within a country will all cause a loss of confidence in an economy. The counterfeiting of money would also have the similar comparison to SWIFT of being a revenue source.

Results from the SWIFT attack are summarised in Table 12 with the full PESTLE analysis in Appendix 7, Table 24. Scores give the best return of effort for the attacker through completing the cyber action. Cyber obtained the highest marks in all categories but for political and technological.

	P	E	S	T	L	E	Total
Cyberattack	2	8	4	0	8	2	24
Insider trading	4	4	0	4	4	2	18
Economic acts	0	0	2	2	0	2	6

Table 12: Summary PESTLE analysis for SWIFT

3.9 Ukraine power grids – December 2015

The attack on Prykar, the second largest electricity provider in the Ukraine, on 23rd December 2015 caused power outages, with a quarter of a million people being left without electricity in freezing conditions [89].

The ‘BlackEnergy’ malware used was spread by hackers believed to be Russian [15, p. 190] and caused substations to be disconnected from the grid. This was achieved through circuit breakers at substations being opened causing the power to be cut [15, p. 193]. The attack also targeted substation converters which meant operators would have to physically travel to the sites to manually to get them back up again [90]. In addition to impede function of the power station the back-up generators were taken out and a kill-disk was used to affect the proper start-up and functioning of computers [15, p. 195].

To increase the psychological element of the attack, a DDoS attack taking out the telephone lines to the power company was also executed [15, p. 194]. This caused panic in the population who, without power and unable to contact the power company, were unable to obtain information on the outages.

Prykar had network segmentation and multiple layers of defence in place so would have assumed a degree of safety against such attacks [15, p. 190]. However, this was a sophisticated attack and used the coordination of many types of malware. Once through the firewall and into the operational systems BlackEnergy allowed manual intervention by the attackers to intervene in the grid's operation [90].

In response to the attack Ukraine attributed the attacks to Russia and began the task of bringing services back online. The response from NATO was to send aid to the Ukraine but did little else to deter or punish Russia [15, p. 302].

A year later, on 17th December 2016, a similar attack on Ukraine's power grid occurred, again believed to be from Russia [15, p. 196]. This attack was even more sophisticated with many components used still unknown, such as how code was delivered to the target. It was also automated, modular and powerful, able to do damage on its own rather than needing an operator. Showing increasing evolution and impact of cyber operations, this left over three million people affected with blackouts [15, p. 197].

Because of its success, these incidents sent shock waves through cybersecurity and government circles. In all imagined cyberattacks, a blackout has always been a big concern of security specialists given the dependency of critical national infrastructure on electricity. In the Ukraine power outages lasted a matter of hours, but if damage had required extensive repair this opening up worrying possibilities of longer timescales.

A view of the US National Academy of Science highlights this risk, 'If a hacker or government shut down the provision of electricity in a Northern city like Chicago or Moscow in the middle of February, the devastation could be more costly than if bombs had been dropped' [91]. The Pentagon's Science Board report claims that the impact of cyberattack shutting down the US energy grid could be catastrophic enough to justify a nuclear response [92, p. 21].

<u>Comparative examples:</u>

Causing a power outage within the Ukraine by a Russian actor can also be done by: (1) turning off the gas supply; (2) damaging a transformer.

(1) Given the gas pipes into the Ukraine are supplied by Russia, these could be switched off causing issues in Ukraine energy supply. Such an instance of the was seen in January 2006 for example [93]

(2) Physically breaking a transformer though sabotage or direct military action would cause long term power outages to a region whilst a replacement was installed. Power grids do not have many spare transformers which are required to steps up or down the voltage in a power grid. These also cost millions of pounds and take a long time to be manufactures and replaced if not within the normal wear and tear replacement cycle [94]

Results from the Ukraine power attack are summarised in Table 13 with the full PESTLE analysis in Appendix 8, Table 25. Scores give the best return of effort for the

attacker through completing the cyber action. Cyber obtained the highest marks in all categories but for economic and technological.

	P	E	S	T	L	E	Total
Cyberattack	8	0	8	2	6	2	26
Turn off gas	0	3	0	4	3	2	12
Hit transformer	4	6	4	2	0	2	18

Table 13: Summary PESTLE analysis for Ukraine power

3.10 US election interference – November 2016

This cyber-enabled information operation by Russia in the 2016 US presidential campaigning raised the profile of the complex links between cyberspace and national security. The techniques used have been compared to the 1960's Soviet idea of reflexive control where the aim is for 'targets to act in the interests of the propaganda without realizing they have done so [95].' Even though this theory is from the 1960's the connectivity of the internet has opened up creative opportunities to execute it.

There has been an evolution in propaganda driven by the nature of online communications. Traditional propaganda would aim to manipulate perception or persuade on one issue with the cyber equivalent now to influence the entire framing of reality. This ability to tailor the message to specific groups or individuals allows the distortion of decision making processes and exploitation their resulting actions. The use of cyber also makes it easier to reach large populations much faster.

Social media provides the ideal platform for this battlespace, containing self-segregated bubbles and echo chambers contesting the nature of reality and truth even without foreign interference. This increases the opportunity for deception and exploiting 'fake news', allowing threat actors to hide in plain sight by mimicking others and increasing ambiguity.

A report released by the US Senate Intelligence Committee released August 2020 concluded Moscow 'engaged in an aggressive, multifaceted effort to influence, or attempt to influence, the outcome of the 2016 presidential election [96]'.

In terms of the cyber operations themselves, the Russian intelligence efforts were well organized, with clear division of labour. Units were separated into specialisms for; developing malicious code, gaining access to targets, mining cryptocurrencies, social media efforts [15, p218]. Russian focus was on 'efforts to hack and leak information to damage Hillary Clinton and the Democratic party [96]'.

As part of the cyberattack John Podesta, chair of Hilary Clinton's campaign, received a spear phishing email, which allowed access to 10 years of his emails, or 50,000 messages in total. Between March and April 2016, 109 more Clinton campaigners got phishing emails, some of which revealed passwords to the Russian intelligence [15, p. 219].

Documents exfiltrated were politically sensitive. Although authentic minor changes were sometimes made, one was forged to show an illegal $150 million donation to her

campaign and another adding a line to her budget indicating anti-regime activities in Russia [15, p. 226].

This attack showed the huge destabilising impact cyberattacks can have on humans and societies. Russian operators boosted messages they wanted American citizens to believe but unwitting citizens and reporters also spread them. Much of the traction that this operation achieved came about because of the subsequent investigations and reporting by non-Russian channels.

The ‘fake news’ campaign was used to drive wedges between key groups in the US using a multi-pronged approach. The cyber operations, with a combination of influence campaigns, interfered and shaped the results of the US election in the opinion of more than a few experts [49], [96].

Even now the 2016 election meddling is shown constantly in the US news which plays into the reflexive control idea. By replaying and propagating the news internally it is creating a self-sustaining operation, generating paranoia and suspicion. The legitimacy of the US administration has been called into doubt, affecting cohesion, leadership effectiveness and decision making processes [97, p153].

The 2016 election, like Stuxnet and the attacks on Ukraine’s power grid, expanded the art of the possible. The impacts became impossible to ignore not only for the meaning in the 2016 elections but also for future elections could be manipulated. Western states started taking seriously the need to protect the democratic processes against foreign interference and fake news.

<u>Comparative examples:</u>

Equivalents to the cyberattack would be actions which could be used to sway an elections. Specifically, I will look at: (1) traditional propaganda and; (2) starting a war.

(1) Propaganda has always existed in society, with media aligning towards the narratives their readers want to hear. In addition to the use of advertising media, other forms including RT media, leaflets, magazines and newspapers.
Unlike social media, these would be publicly open channels with a generally traceable narrative that would not disappear into the ether when read.
Crucially, advertising funds used would be auditable so it would both be possible to attribute the messaging to a given party or identify if electoral spending regulations were adhered to, in contrast to the social media landscape.

(2) It is widely accepted concept that when there is a risk to national security the American electorate gravitate towards the party of defence, the Republicans. The Republican party typically have a more hawkish stance than the Democrats, so would be favoured when the defence of the US maybe under threat.
As such, Russian posturing and shows of force (flying into US airspace) even temporarily during the election cycle in 2016 could have pushed the narrative towards a more Republican agenda. This could have impacted swing votes sufficiently to have gotten Donald Trump.

Results from the US election attack are summarised in Table 14 with the full PESTLE analysis in Appendix 9, Table 26. Scores give the best return of effort for the attacker through completing the cyber action. Cyber obtained the highest marks in all categories but for technological and economic.

	P	E	S	T	L	E	Total
Cyberattack	8	4	8	2	6	1	29
Propaganda	4	2	4	4	3	2	19
Start a war	0	0	0	4	0	0	4

Table 14: Summary PESTLE analysis for US election

3.11 WannaCry – May 2017

On 12th May 2017 a cyberattack called WannaCry crippled IT systems across the globe in the biggest known ransomware outbreak in history. It quickly spread across 150 countries, infecting hundreds of thousands of computers, encrypting their files and locking out their users. In total it caused approximately $4 billion in damages and had a destabilising effect on businesses who were worried about plugging devices into the Internet in case they became infected [15, p. 278].

Although a technology flaw in the Windows operating system made the attack possible, a patch for this had been available months beforehand [98]. Users who had installed patches had up to date software and were unaffected but those who did not were vulnerable.

WannaCry had a particularly serious disruptive effect on National Health Service (NHS) hospital trusts within the UK. To recover cost the NHS £92m and resulted in 19,000 patient appointments being cancelled. The attack affected at least 81 of the 236 trusts across the UK, either directly or indirectly, in addition to 603 primary care trusts and GP surgeries [99].

NHS Digital suggested that hackers were not able to access patient data and reportedly no harm was caused to patients [100]. However, urgent NHS services were hindered during the attack. Some trust were forced to divert ambulances and A&E departments sent patients to other hospitals [99].

In addition to preventing access to computers, the cyber-attack also locked out important medical equipment such as MRI scanners and devices for testing blood and tissue samples. More than 1,200 pieces of diagnostic equipment were infected by the ransomware, with many more disconnected from IT systems to prevent spreading the infection [15].

The attack raised serious questions about the preparedness of the NHS to deal with such incidents. An Government Audit Office report concluded that if basic IT security practices had been followed, updating firewalls and migrating to newer computers, the attack could have been prevented [101]. The NHS have since taken steps to ensure better security and incident response in case of future issues.

WannaCry has been attributed to the North Korea, who used tools and malicious code released online which had been stolen from the NSA [102]. The aim of the attack is thought to have been the disruption of businesses around the world and a way to make money from the ransomware – although few payments were made.

The crippling effects of WannaCry on the NHS bought into clear perspective that fatalities as a second-order consequence of persistent and large-scale cyberattacks 'may not be far behind [48, p. 238].' The release of hacking tools also made the cyber realm much easier for malicious hackers to infiltrate systems, with the toolkit of the most advanced cyber nation at their disposal.

Comparative examples:

Examples used to compare cyber with traditional attack are: (1) creating doubts in records and; (2) destroying a data centre.

1. An employee placed within a Healthcare Trust could easily enter data records incorrectly and change existing information. Over many months thousands of records could be changed with lack of visibility as to which records have been falsified. This could result in operations being cancelled within the Healthcare Trust due to records not being trusted. If patient blood type had the possibility of being incorrect for example it would be considered irresponsible to operate without repeating tests. Confidence in the service would fall significantly with the NHS flooded with having to duplicate of tests.
   Additionally, with 18 million people in the UK having a long term medical problem [91] there could be the need to re-test and validate records of up to 30% UK population. This is assuming the accuracy of medical histories is most important for these groups and those undergoing active treatment.

2. Data centres would hold patient records so destroying this would again create large scale disruption from the same logic mentioned in attack (1).

Results from the WannaCry attack are summarised in Table 15 with the full PESTLE analysis in Appendix 10, Table 27. Scores give the best return of effort for the attacker through completing the cyber action. Cyber obtained the highest marks in all categories.

	P	E	S	T	L	E	Total
Cyber	4	4	8	4	6	2	28
Records doubt	0	0	4	0	3	1	8
Data centre	2	8	0	4	0	0	14

Table 15: Summary PESTLE analysis for WannaCry

3.12 Conclusion

Work completed with the PESTLE framework has allowed detailed comparisons between individual attacks realised with cyber means and theorised comparable physical alternatives. Working papers from the PESTLE analysis are given in Appendices 1-10, Tables 18-27. The ten case studies have been scored based on

assessing the most promising outcomes from the point of view of an attacker. The higher the score the higher an attackers return on efforts for their costs incurred.

PESTLE data from the attacks within Sections 3.2 – 3.11 have been combined in table 16. This allows comparisons to see if patterns emerge in use cases across cyberattacks, lower impact kinetic options and higher impact kinetic options.

As can be seen cyberattacks score highest in total across all the three types of attack analysed – cyber, low kinetic effect and high kinetic effect. Cyber scores particularly highly in the political arena with technological scores being very low due to the newness and complexity of the apparatus and arena.

	Estonia	Georgia	Stuxnet	Aramco	IP theft	Sony	SWIFT	Ukraine	US election	Wanna Cry	Total
Political											
Cyber	8	8	8	6	8	8	2	8	8	4	68
Low kinetic	4	4	0	3	4	4	4	0	4	0	27
High kinetic	0	0	4	0	0	0	0	4	0	2	10
Economic											
Cyber	0	6	0	8	8	6	8	0	4	4	44
Low kinetic	6	3	6	4	4	3	4	3	2	0	35
High kinetic	3	0	3	0	0	0	0	6	0	8	20
Social/cultural											
Cyber	8	4	6	6	0	8	4	8	8	8	60
Low kinetic	4	8	0	3	3	0	0	0	4	4	26
High kinetic	0	0	3	0	6	4	2	4	0	0	19
Technological											
Cyber	0	0	0	0	2	0	0	2	2	4	10
Low kinetic	4	4	3	4	4	2	4	4	4	0	33
High kinetic	2	2	6	2	0	4	2	2	4	4	28
Legal											
Cyber	2	6	6	6	6	4	8	6	6	6	56
Low kinetic	0	3	3	3	3	2	4	3	3	3	27
High kinetic	4	0	0	0	0	0	0	0	0	0	4
Environmental											
Cyber	1	2	4	4	2	2	2	2	1	2	22
Low kinetic	1	1	2	2	2	2	2	2	2	1	17
High kinetic	0	0	0	0	1	2	2	2	0	0	7
Total											
Cyber	19	26	24	30	26	28	24	26	29	28	260
Low kinetic	19	23	14	19	20	13	18	12	19	8	165
High kinetic	9	2	16	2	7	10	6	18	4	14	88

Table 16: Combined PESTLE analysis

4.Porter’s Five Forces analysis

4.1 Introduction

When applying Porter's Five Forces to the cyber weapons arena we are considering how the marketplace for the specific attack behaves. The Porter's framework makes us consider the different competitive forces which would ultimately make an attacker decide if the cyberweapon was the most efficient and economical to deploy, or even feasible to develop.

This has been approached from the point view of the cyber weapon developer. To understand how the competitive dynamics differ across the attacks three levels of sophistication have been considered. These represent the broad levels of technical skill and capabilities observed with the different attacks analysed, and are defined as:

1. High complexity and specificity: Multiple, complex or rare, components are required to function. For example, the Stuxnet and WannaCry case studies;

2. Medium complexity: High skillsets or agility in infiltration; potential manipulation of target to deploy; fewer components required to function. For example, the Sony Pictures, Saudi Aramco, Ukraine power grids, SWIFT, and F-35 IP theft case studies;

3. Low complexity: Pre-existing toolkits, or widely available services available. For example, the Estonia, Georgia, US election interference case studies.

WannaCry has been placed on the high complexity side due to the nature of the exploits used, that the attackers had used stolen tools and were likely unable to develop it themselves should not detract from the original complexity of design.

4.2 Threat of substitute products

This category covers how likely it is that there would be another means of achieving your goal, either completely or in part. It is noted that only substitute products through cyber means will be considered here, with those outside of the cyber realm being extensively covered in the PESTLE frameworks in sections 3.2 - 3.11.

High Complexity

With highly specific targets (Stuxnet) or the ability to create significant, cascading, disruption across networks (WannaCry) there are few other cyber products which would meet these needs. These products tend to be very specific and are not substitutable, i.e. one product equals one principal target. With a need for automated deployment and finding the targets across a wider network these products cannot be swapped out easily or by a part cyber, part manual solution.

Summary: No substitutable products are available

Medium complexity

With more open targets, which often bring additional weaknesses, and often having a lag between the initial deployment and actual incident, these attacks are less complex than the first group. Additionally, once present within the network information may be slowly fed back, allowing the attacker to build up an enhanced view of the network and its further weaknesses. The majority of these attacks could have been achieved through similar, but alternative, cyber means and also relied more heavily on external system weaknesses (management and human) to achieve their goal.

Summary: Moderate substitutability, but options remain complex to deploy

Low Complexity

Products and toolkit and openly available. Within Estonia, a large part of the attack was delivered by script kiddies using easily downloadable tools. The US election interference was run over a public platform which allowed data mining and targeting; such targeting is possible with common machine learning algorithms.

Summary: Products can be substituted to alternative tools and / or models

4.3 Threat of protection versus attack

Within the business world the threat of new entrants discusses how robust a business is against external threats. If a new entrant could arrive easily then any investment that has been made is vulnerable and any future gains are expected to be less than if a new entrant hasn't materialised. Within the cyber weapons field this has been re-purposed to be the 'threat of protection versus attack', i.e. how likely and suddenly could the techniques used become defended against and rendered obsolete.

High complexity

Attacks such as Stuxnet required multiple zero-day vulnerabilities to function successfully. Had any of these been patched in the weeks prior to launch the attack would likely have failed. With Stuxnet taking many months to deploy and sitting on target servers un-noticed the risk to the operation of such patches being released will have been independent of the attack, and reliant upon a security company identifying and fixing the vulnerability.

With WannaCry the situation was different in that once the attack was released, researchers began looking for means to both slow and neutralise the spread. Review of the code will have highlighted the exploits used, therefore which were the vulnerabilities to patch quickly. As such the deployment of the weapon itself results in the closure of the exploit required for propagation.

With zero days being considered rare – but with frequent examples of independent discovery soon after initial find [57] – each day brings a greater risk for the attacker that the weapon will no longer work. Once the exploit is exposed it becomes a question of when it will be closed on the specific machines being targeted.

Summary: Threat of protection versus attack high; utilisation will lead to protection

Medium complexity

These attacks lack the number of zero day exploits that more complex attacks rely upon or are attacking systems which are either harder to, or generally, never patched. For example vulnerabilities in computer operating systems are frequently updated, whereas outside of Apple mobile phones (iOS) there are fewer updates, with the majority of Android handsets running on out of support software [103].

Additionally, with a known weakness in either the software or the interfaces it is possible for the performance of the attack to be monitored and changes within systems made to prevent discovery, extending the life of the attack.

Generally these attacks require improvement in defensive strategy, such as closing gaps in physical as well as information systems, which are less coherently applied globally.

Summary: Medium risk of protection versus an attack developing

Low complexity

Most of the lower complexity attacks are based upon one of three different methods:

1. Brute force attacks such as DDoS which, if you have enough computers at your disposal are cheap and effective and can be performed by low-skilled actors;
2. Use openly available toolkits to attack hard to patch weaknesses, such as open access points. To prevent these it requires that a user is aware of the network security, such as in Internet of Things (IoT) devices, however usually they are unaware of the risk – such as default, hard coded passwords;
3. Relying upon exploits within the human system. For example Facebook looking to drive advertising revenue without checking the origins or contents of advertisements on its platform. People clicking on misleading links can be inadvertently downloading the attack device itself.

Many of these attacks require weakness in the overall system, not just the cyber aspect, to succeed.

Summary: Low to no threat of protection; methodology can be used repeatedly without risk of immunity being developed

4.4 The power of buyers and the power of suppliers

These two aspects have been considered together within analysis due to the nature of the products. Given cyber capabilities appeal to both the white hat and black hat market for different reasons this creates an interesting power dynamic which is more nuanced than could be expected.

For clarity, ‘buyers’ refer to those procuring the components of the cyber tools for use, ‘suppliers’ refers to those looking to provide them.

High complexity

Within complex attacks the dynamic between buyer and supplier is highly nuanced, depending on the ultimate aim of the attack and the priorities of the nation state. To bring out these nuances two different areas of a complex cyber weapon will be bought out separately: zero days and; computer scientists and developers.

1. Zero Days: The market for buying and selling zero days is opaque, with sellers either offering them to the manufacturers or for sale on the dark web. On the dark web, closed auctions will place power in the supplier hands. Given the buyers will be unaware of the amount being offered by competitors, they will be forced to overbid if an exploit is crucial for their weapon design.
   However, this dynamic changes when the state is not only the buyer, but also the identifier of the zero day. Rather than make the manufacturers aware of the problem it may, as a buyer, decide to instead withhold knowledge to incorporate in its own attacks. By claiming national security the buyer is able to supress the suppliers power. As noted in Section 2.13, the US use 'The Vulnerabilities Equities Process' to determine whether to disclose a vulnerability or not [58].

2. Computer Scientists and developers: Specialised, highly proficient IT experts are few and far between, even more so where security clearance is required, Given the skills required to develop and deploy cyber weapons are scarce, this pushes up the cost of these individuals.
   Government, however, have the benefit of being one of the few employers able to offer cyberattack and national security roles which will attract certain individuals and help to balance the compensation challenges which they face with the technology industry. This only extends so far though, with patriotic talent moving out of the government for higher pay packets being contracted back to do similar roles [49].
   The ability of some states, such as Russia, to co-opt those actors known to be using cyber skills for illegal gains highlights the extreme power the buyer (state) can ultimately wield if required.

Summary: Overall balance of power to suppliers, but the power of buyers is strong when there is government backing

Medium complexity

Medium complexity attacks again usually require both cyber and physical operations to deploy successfully. Instead of using zero-days, these attacks often using known exploits combined with behavioural observations in how systems are used. The skills and knowledge of the attacker is of vital importance – even if a public toolkit is being used, the ability to remain undetected and knowing how to erase ones tracks in the target system is still required. This increase in skill and systems knowledge places the balance of power towards the supplier.

In contrast to the highly advanced attacks which require state backing, and patriotism or coercion, these attacks tend to be more at the edges of state sponsorship. As such

the buyer does not have the same level of power and therefore patriotism or control over the actors.

Similarly, if zero days are required, given other options exist it is unlikely the state would themselves hold knowledge of them back from the market. It would thus be required to use 'traditional' purchase channels, increasing the cost and supplier power.

Summary: Overall balance of power to suppliers

Low complexity

With techniques either already in the public domain or low skill supplier power is low at this end of the cyber spectrum. It is often even performed for free by individuals looking for patriotic reasons or in order to demonstrate a willingness to progress within the enterprise.

Where the attackers are procuring goods and services, such as advertising, email accounts and followers, those supplying the services are unaware of the real value of these to the buyers Therefore, within an open-market environment, suppliers will generally under-price.

Summary: Overall balance of power to buyers

4.5 Rationality of the market

This category refers to how different competitors within a marketplace respond to actions by others which change the competitive landscape. For example, if one actor drops the price of a product, do all the other actors in the marketplace follow this drop in price.

High complexity

With complex cyber weapons being the preserve of nation states there is a natural bias towards being in control of superior armaments to your opponents. This is apparent within the re-purposing and intensifying of medium complexity attacks such as Saudi Aramco.

Lack of rationality is also apparent within the retention of zero days for cyberattack purposes which leaves the wider population at risk from significant disruption. WannaCry exemplifies this with the core attack having been obtained from the NSA. Had the US government patched key vulnerabilities it was aware of, one of the most disruptive attacks perpetrated so far would not have been able to occur – nor high end toolkits be available open source to download [104]. Some countries believe patching these vulnerabilities is the more rational thing to do [105].

Summary: Borderline irrational but a lack of visibility prevents a full blown arms race

Medium complexity

To date, August 2020, there have been limited public escalations of cyberattacks with aggressors facing little in the way of sanctions or major retaliation. These do exist,

such as economic sanctions against North Korea for the Sony hack, but are few and far between. Given the potential damage and unintended consequences which could arise from a rapidly escalating series of cyberattacks, this 'restraint' is being viewed here as signs of operating within a rational market.

The majority of mid-level attacks have focussed upon short-term, reversible, damage as opposed to longer-term blackouts, disruption and attacks upon core financial and support institutions. This again demonstrates a degree of rational restraint within this space. This appears to be driven more by uncertainty and fear of escalation however than a calculated decision.

Summary: Borderline rational driven in part by fear of escalation

Low complexity

At the simpler end of the cyber weapon and attack spectrum the rationality of the market falls into two distinct sections:

1. The cyber element is rational. Hardware and software manufacturers continually review means to protect against exploits, creating updates and patches based upon the risk created versus the complexity to exploit and damaged caused;
2. The human and emotional side of any attacks is borderline to fully irrational. Consumers who bemoan the power and influence of the technology giants continue to fuel their growth with more and more information and buy into their stocks as they continue to grow in value. The concept of ‘too good to be true’ is continually ignored as people click on dubious links creating easy ways into systems.

Summary: The cyber element of the market is rational, the human element is irrational

4.6 Conclusion:

Work completed in the Porter’s Five Force’s framework has allowed consideration of different competitive forces which would ultimately make an attacker decide if the cyber weapon was the most efficient and economical to deploy, or even feasible to develop. This was completed across high, medium and low levels of attack sophistication covering the ten attacks considered.

A summary of the findings are shown in Table 17. As can be clearly shown there are distinct market segments depending on the complexity of the cyber weapons being considered.

	High complexity	Medium complexity	Low complexity
Threat of substitute products	No substitutable products available	Moderate substitutability, but options remain complex to deploy	Products can be substituted to alternative tools and / or models
Threat of protection vs attack	Threat of protection versus attack high; utilisation will lead to protection	Medium risk of protection versus attack developing	Low / no threat of protection; methodology can be used repeatedly without risk of immunity developing
Power of buyers / suppliers	Overall balance of power: suppliers, but buyer power strong with government backing	Overall balance of power: suppliers	Overall balance of power: buyers
Rationality of market	Borderline irrational – but lack of visibility prevents full blown arms race	Borderline rational – driven in part by fear of escalation	Cyber element of market is rational; Human element of market is irrational

Table [17]: Summary of Porter's Five Forces analysis

5 Conclusions

5.1 Conclusion

Across all of the attacks reviewed the cyber option was the strongest in each case (joint strongest in one case), often by a considerable margin. Given that known cyberattacks were chosen for analysis this is far from surprising with preferences revealed in awareness of only successful cyberattacks. Also it would be a sensible assumed that governments would have completed analysis to compare traditional and cyber weapons before a deciding to deploy the cyber option. However, the reasons behind the superiority of the cyberattack differed across the scenarios.

In some cases, cyber was a slightly better way of achieving an effect a state could have achieved otherwise. In other cases, cyber created opportunities that realistically did not exist before. This highlights a series of both strengths and weaknesses, as well as how cyber is changing the very nature of what it means to be 'at war'.

5.1.1 Cyber changes the battlefield

Across the vast majority of the kinetic options for the ten attacks there are two key elements in common.

1. They require nation states to send troops or agents into a foreign country to carry out physical activities against that state, or to launch missile attacks against them
2. There would exist physical evidence linking the act back to the aggressor – flight paths, munitions casings, standard operational fingerprints, a money trail

Within the cyberattacks none of these were found with sufficient uncertainty that attribution, although made, remains probabilistic and not absolute in most of the attacks. Crafted and deployed many miles away, no agents set foot on foreign soil to deploy them. Instead the front line moved from where the targets were located to a computer terminal in Virginia or North Korea with traceability more difficult.

The lack of attribution and ability to launch attacks from anywhere are not the only changes. What is, and is not, fair game to attack is also changing, as are the recruits and new soldiers in this 'war'.

With the cyber world not 'owned' or 'maintained' by the government the range of targets has grown. Major corporations have become a focus of the attackers looking cause disruption and influence policy. It would be inconceivable for a nation state to launch a kinetic attack on a publicly listed company in peacetime, but we have observed such multiple attacks within the cyber world, Saudi Aramco and Sony Pictures for example. With the ability to withhold service as opposed to destroy, attacks on core utilities which give only a temporary effect are now options as well.

The attack on Saudi Aramco, caused the oil distribution of oil within the country to be halted for 17 days [71]. Sony Pictures showed a clash of autocratic and democratic regimes. Although an attack on a private company, the attack took on political meaning with the US President stepping into the fallout calling on Sony not to give into the demands of a foreign dictator [15]. Not only was the free speech of the US seen as

undermining the divine ruler of North Korea, the North Korean leader was seen to be undermining US freedom of speech.

Actors within the cyber ‘frontline’ are fundamentally different those seen in the past. Complex attacks require the exploitation of flaws within widely used operating systems we all rely upon for everyday life. Infantry soldiers are being supplemented with botnets and script kiddies which are unaware of what the real political implications could be and too numerous to capture. Although you could say this to an extent of the infantry, a long period of training provided before service and there is a sense of battlefield cause and effect still present. Within the attack on Estonia script kiddies were mobilised in short time periods through Russian websites, where exploits could be downloaded in ‘plug and play’ attacks.

Finally, with every computer being a potential attack vector, the threat of cyberattack is redefining the social contracts we all need to uphold. At an individual level, everyone needs to be able to protect their devices to ensure that they are not taken over for the use in malicious attack, as part of a ‘bot’ or a way to get inside a corporate system for example.

At a governmental level, this may takes the form of being responsible in disclosing zero days to software developers so that they can be patched to ensure the security of everyone, rather than held for attack tools. Or conversely holding onto these attack tools, to increases government intelligence and covert action capabilities, enabling the defence of national, ensuring the security of everyone.

Areas which are ‘off-limits’ also require defining and protecting under international law. Barack Obamas cited that one such area is the financial sector, such as the SWIFT system targeted in one of the examples.

5.1.2 Areas where cyber is beneficial

As discussed in Section 5.1.1, cyber operations are attractive precisely because they exist in the shadows, revising the distribution of power and allowing deniable action at a distance. Indeed, the most fruitful cyber operations may not have yet discovered their covertness being part of the measure of their success.

Like air-power, cyber weapons allow nations to ‘engage in hostilities by increments', [15, p. 154] but without causing significant damage that makes reconciliation more difficult. As cyber weapons generally inflict harm short of traditional war, they expand the choice of options and outcomes available to an aggressor.

Based upon my analysis of the ten attacks there are three key strengths which make cyber operations very attractive for military and political purposes.

1. They can combine action at a distance with close quarters accuracy and efficiency, permitting a new class attacks which are de-risked through remoteness.
   Both the Stuxnet and Sony Pictures attacks benefited from this with the attack able to infiltrate what would normally be well physically protected sites. Once inside the attackers could, in the case of Stuxnet, destroy the targets as effectively as a precisely placed explosive charge, yet with none of the detection

and capture risks. With Sony the attackers had their choice of documents to release and leak to cause maximum damage. In the physical world this is equivalent to slowly checking all the filing cabinets and moving office to office to find the best items to steal.

2. They offer the ability to strike rapidly, without warning across an entire network, propagating faster than the investigators can react to, or be aware of.
   When the Shamoon worm was unleashed at Aramco it hit completely without warning and within hours had taken over the network, wiping out computers as they connected. Engineers resorted to physically unplugging any devices they could find in order to defend across the multi-site corporate network [68]. Few kinetic attacks are able to spread so rapidly from a standing start to hit targets in so many different locations. The same was true in the Ukraine, where multiple sites in the power grid were hit simultaneously.

3. Effects can be reversible and limited in duration. For many of the attacks analysed, the intent was to demonstrate that the aggressor had the power to create problems but not to destroy infrastructure permanently.
   This is highly attractive for two reasons. Firstly, if you were looking to invade a country, as with the Russian invasion of Georgia, by not destroying the communications networks you are then able to use it yourself once in power. This reduces or avoids any future costs and ensures no power vacuum exists for others to fill outside of your control. Secondly, by stopping short of actual destruction, the level of retaliation accepted within the international arena falls dramatically, Russia was condemned by NATO for the strikes against the Ukraine but little more, avoiding any further escalation.

Although some governments and militaries have had longer term experience of dealing with cyberattacks, many have not. Within the high level policymaking, public debate, the legal environment and setting typical standards there is less understanding still. This, affects the legitimacy, cohesion and effectiveness of the political decision making processes through institutions and leadership can be undermined. This can be by either buying time for a physical operation to succeed before an adversary can respond or by raising doubts in the process itself.

For the defender it is difficult to cover all the attack surfaces. However, the non-destructive element does provide some benefit with computers and impacted areas usually able to be reused after the attack has passed. Contrast this with missile strikes which cause large rebuilding projects to be undertaken on damaged building and equipment.

5.1.3 Challenges of deploying cyberattacks

Whilst cyberattacks were overall the strongest means of achieving aims of the attack, scores for the cyber weapon were lowest within the ‘technological’ category. This was due to the degree to which, for the more complex attacks, the weapon had to be carefully tuned to the target, approaching a one-weapon-to-one-attack basis.

As a new field, the capabilities and expertise needed to construct a weapon are still much more specialised than in the kinetic examples studied, where technology is mature with more examples of its use in the field. This technological gap is likely to reduce in the future, however, as more cyber weapons are used in the field and a growing amount of research and experience is built up.

It is, however, noted that some traditional weapons outside of the case studies covered in this report would have extremely specialist research and development too, such as hypersonic technology and directed energy weapons for example.

When comparing the weaknesses of the attacks and the market dynamics five main challenges within cyber stand out.

1. Highly specific cyberweapons balance destructive capability against containment challenges and fragility. In order for an exploit to be used by the state, the vulnerability needs to be unpatched when the attack takes place. With some attacks requiring multiple zero-day exploits, this places both the feasibility of the attack and the attacker themselves at risk, as the vulnerability could be fixed, or the exploit be used against their country.
   Specificity and containment of cyber weapons are major issues and there are parallels with early aerial bombing campaigns during World War II. These air raids often caused unwanted escalation in civilian domain bombing given the lack of targeting and caused unpredictable amounts of damage [3]. Like these bombing campaigns, cyber weapons, particularly at the lower end of capabilities, can cause indiscriminate disruption. As the WannaCry case study showed, a cyber weapon which is let loose to spread across the globe can cause devastating damage at an alarming speed. The challenge for nation states would be to ensure attacks are contained and targeted so as not to cause unwanted escalation and destruction. Some states appear to put a lot of effort into this, as observed in the Stuxnet example, whilst other states seem less risk averse, as seen with WannaCry.
   A terrorist would not be this considerate, however, so there is also the challenge of defending against such attacks as well as less sophisticated attackers of any kind who do not understand the implications of the tools that they deploy. A general tightening of security among businesses, scared into action by companies such as Saudi Aramco being targeted, is causing some of the easy ways into systems to be secured. This increase in security is counterbalanced, however, by an increase in weapons capability being released onto the market, most notably the Shadow Brokers releasing tools they stole from the NSA.

2. Unlike other forms of weapon, cyber weapons can rarely be executed on a one touch basis. Almost all of the attacks analysed needed some form of human misdirection to persuade someone to click on a link or plug in a device for example [106], along with monitoring over many weeks once live. This is in contrast to many kinetic weapons which, once released, are live with little additional monitoring or guiding required, so called ‘fire and forget’ weapons.
   Additionally, the existence of the code does not in itself create the results. In the case of the US election interference and targeting on social media, cyber

does not remove the need to develop the underlying content and messaging for distribution, it merely simplifies the targeting and delivery. However, the fact that cyber does create these possibilities has transformed the ability to reach out and influence groups of people and get material to them faster and more cheaply than would have been the case before cyberspace.
Within the SWIFT attacks the cyber aspect provided the means to steal funds, the actors themselves having to create the transactions over time.

3. Speed and cost. The costs of deploying cyber weapons is deceptively high when specificity and capability level is increased. Stuxnet took many millions of dollars to complete with levels of testing which included replicas of the Natanz facility to ensure not only working of the cyber weapon but to ensure that it did not spread to other systems [49]. Even with these costly precautions, Stuxnet did end up spreading onto machines outside of the Natanz facility.
Cyber weapons can take months to create and fine tune . Even a simple DDoS attack requires the infecting and recruiting of devices to perform it, so once used and identified it is not just as simple as 'copying and pasting' capabilities.

4. Cyber weapons are best suited for pre-meditated attacks, not rapid response or as a defensive means within combat. Whilst they can be deployed very quickly, this is only after a period of reconnaissance, development and planning, which, depending on the target, could take many months.
Whilst it could be argued that attacks such as WannaCry could be used within a defensive capacity were another state attacking you, given the limited lifetime of an exploit once released you are unlikely to have many such weapons to use and it would be an act of last resort. Also there is only so much that a cyberattack could achieve once for example tanks had started to cross into your sovereign territory.
This presents a stark difference between the kinetic and cyber worlds. The majority of kinetic weapons function in both an aggressive and defensive purpose.

5. Once launched, technology effectively becomes open source. As Iain Lobban, former Director of GCHQ, states 'What was considered a sophisticated cyberattack only a year ago might now be incorporated into a downloadable and easy to deploy Internet application, requiring little or no expertise to use [67]'. Not only have the Shadow Brokers released attack tools but once the Stuxnet code was analysed it was made open source and used in subsequent attacks. More broadly, once code is used it can be analysed and re-used, which is a challenge for escalation effects in the cyber domain and a key difference to conventional weapons.

5.1.4 Cyber weapons are here to stay

The global cyber weapon market was valued at $45.12 billion in 2018, with this estimated to be worth $65.13 billion by 2027 [2]. This growth is driven by an increased

need for cyber security, with the rise in the number of cyber issues and the need to secure critical national infrastructure. There has also been a rise in defence spending, an increase in the use of cyber weapons and demand for advanced cyber weapons which are driving the market – with traditional arms manufacturers increasingly expanding into cyber space [2].

Spending increases in this sector, as well as the huge numbers of connected devices projected going forward, implies that the cyber weapons market is not going to disappear. Individuals, governments and the military will have to get better at securing devices in order to stay ahead of attackers.

5.2 Further work

When researching cyber weapons so many other areas have been found which could form fields of further study. Intricacies within the cyberspace domain make them quite distinct from the other four domains, with many of these intricacies still needing to be untangled.

As mentioned in Section 2 there are many ways in which cyber weapons differ from traditional weapons. Issues of attribution requirements and ways to prevent proliferation were covered along with cost analysis required to determine accessibility for actors. These issues will not be discussed again here but are all areas in which further work can be done. Other areas worthy of further time and study will now be discussed.

Escalation

As we have seen when analysing the Stuxnet operation, targeting an Iranian nuclear enrichment plant with a missile strike could kill many people and cause radioactive contamination, giving the Iranians a strong incentive to escalate in retaliation. In contrast, using a cyber weapon gave much lower collateral effect on both property and human life, reducing escalatory incentive whilst also delaying Iran's nuclear programme. However, in some scenarios cyber weapons could be more escalatory; if critical systems failed during a crisis situation due to an accidental coding error but this being misinterpreted as an attack.

The attack on Saudi Aramco in 2012 was seen by Iran as responding to an earlier attack on their energy sector [69]. However, the US interpreted the attack as 'a significant escalation of the cyber threat [107].' In this situation the attack used by Iran was near identical to that used by Israel, yet still misinterpreted as escalation with others not recognising the prior attack, or maybe choosing not to recognise the prior attack to paint Iran in a poorer light. This shows just how easily a situation can get out of control in the cyber domain in which one side sees itself as acting proportionately and the other seeing the action as escalatory.

Cyber weapons open up more ways to escalation but also give opportunities for control. Finding the balance between showing resolve but not giving an opponent the incentive to escalate needs close work to avoid inadvertent escalation. It is presumed governments are attempting to formulate policies to address this, however, it is not

known for certain given a lack of openness as compared to say the arguably open discussions of nuclear strategy in the Cold War. In cyber, the academic discourse may be lagging behind practitioners' discussions so future work could be to better understand how these questions have already been answered in practice.

Unintended consequences

Within a complex system such as the Internet it is difficult to just do one thing, 'multiple parties and stages permit many paths to unanticipated consequences [107].' Within the analysis completed an assessment of the unintended consequences was touched upon, with events such as political fallout, setting up of cyber defence leagues, or the writing of the Tallinn Manual some examples of this.

In further work it would be worth looking closer into these unintended consequences, with say a risk assessment completed as to the likelihood of these second or third order events so decision-makers can more fully assess the likely consequences of their choices.

Role of non-state actors

Ben Buchanan states that the biggest difference in the cyber domain is the private sector's role, rather than speed or attribution of cyber, with governments not holding the levers in cyberspace needed to solve cyber conflicts [55]. In many circumstances governments need to work with the private sector, given the latter's agility and subject matter expertise in this arena. Indeed, the private sector also own most of the networks within this domain, with 85% of US critical infrastructure being in private hands [20, p. 99].

It has been noted from within the US that the federal government should not dictate solutions to the private sector [108] nor should it 'secure the computers of privately owned enterprises such as banks, energy companies, transportation firms, and other parts of the private sector' [109]. However, solutions to the issue of national security concerns sitting with private companies need to be found.

Hack back

Within Britain and the US the authority to use offensive weapons is exclusively that of the government [3, p. 230]. Notably in the US there have been calls to allow companies to 'hack back' against network intrusions, essentially arming civilians in cyberspace. This has been so far rejected by the courts, but it would appear that even without a law in place companies are using 'hack back', with a poll 36%, of 181 companies polled in 2012, claiming to have done this [3, p. 236].

There would definitely be benefits for the defender in being able to go after offenders not only within their networks, but pursuing them across cyberspace. However, these benefits would be balanced by an increase in risk to innocent parties through being caught in the 'cross hair' of retaliation, through incorrect attribution. Moreover, the cover of 'hacking back' could be misused as a way to settle business grievance. There is also the issues with this at a global scale too, with greater risk of international conflict.

If hacking back were to be made legal there would need to be work completed - ideally beforehand – into consequences of this on a micro and macro scale as well as strategies developed to deal with this significant change.

IoT

With the number of 'things' connected to the Internet set to increase significantly in the coming years these give countless new attack vectors with which to penetrate networks. Driverless vehicles, city 2.0 and industry 4.0, as well as connected homes and personal devices, will need to be modelled within the international arena to assess the vulnerabilities of these to cyberattack.

Deterrence

Decades of research have been conducted by strategists and analysts on traditional weapons deterrence [107, p. 175]. Deterrence is key for conventional military weapons such as aircraft carriers, fighters and jets and not only for nuclear capability. It shows your power to your enemies so they won't attack you.

The situation with cyber deterrence is different as discussed in this report, there are no 'May Day' parades for cyber to flaunt capability. There is a lack of visibility to show who is best in cyber power, military budgets shows countries such as the US Israel, Russia, China, Iran and North Korea are spending money but there is no visibility for on what [33].

As Martin Libicki states, 'brandishing a cyberwar capability, particularly if specific, makes it harder to use such a capability because brandishing is likely to persuade the target to redouble its efforts to find or route around the exploited flaw [110].' Cyber is a threatening capability which, when revealed, gives to the opposition knowledge of how it can be neutralised. Deterrence in this domain may in fact look like the attack on Estonia, this being a demonstration of capability by Russia for example.

Combined effects

'Cyberwarfare is routinely overhyped as a new weapon of mass destruction, but when used in conjunction with actual weapons of mass destruction (WMD) there are severe and underappreciated dangers [111, p. 205].' A combination of nuclear credibility and cyber deception would not mix well. An attacker who infiltrates an adversary's nuclear command and control for example will not be able to communicate their advantage without the other side being able to find the infiltration and patching it. The adversary will continue to believe it wields a deterrent that may no longer exist, and their opponent knows this [111, p. 206].

This report looked at individual cyber weapon, with combination of attacks across cyber and kinetic worthy of investigation to understand their dynamics.

Single versus multiple usage

Tactical uses of a weapon, either cyber or kinetic, focus on short-term, narrow goals like the defeat of an adversary in the neighbouring village tomorrow. Strategic uses of weapons, by contrast, focus on longer-term, more overarching goals and are designed

to affect the broader dynamics between potential adversaries both on and off the active battlefield.

Within the four domains of kinetic warfare there is a suite of tools, vehicles and divisions which permit the entire offensive to be run as a single, continuous campaign. Finding out what this looks like within the cyber domain, which presently appears to be consist of individual, targeted attacks would be worthy of investigation.

5.3 Closing thoughts

The best way to conceptualise cyber weapons appears to be through concepts of espionage, sabotage, and destabilization rather than kinetic effects [15 p. 8]. These actions are usually treated as tools of state-craft which are accepted as par for the course by countries internationally and not a reason to escalate to war.

Cyber weapons may not produce the physical destruction and loss of life traditionally linked to the waging of a war, but they are having significant impacts. In 2018 US Cyber Command acknowledged this strategic significance of below-the-threshold engagements in cyberspace required in order to compete successfully [27, p. 9].

It has been noted, each loss of IP and trade secrets through cyberattack maybe too small to be fatal individually but as they accumulate it could create significant consequences and cripple a country [49]. ‘We should not forget that it was from China where 'death by a thousand cuts' originated [26, p. 94].’

In 2016 the US Republican Party stated, ‘Russia and China see cyber operations as a part of a warfare strategy during peacetime [112].’ Others, including Fergus Hanson have also described the phenomenon of ‘Waging (cyber)war in peacetime [113]’.

There does seem to be something unique about cyber weapons. The economics, politics, and fabrics of societies are being changed with effects noticeable in the real world much like their physical counterparts, rather than opaque spying operations of espionage. It seems simultaneously like peace and war at the same time, a kind of quantum state of both possibilities simultaneously. As stated by Lucas Kello:

‘The Clausewitzian notions of war and peace are polar binaries with the notion of peace failing to capture the strategic problem and the definition of war highly focussed on physical damage. A lot of the activities done in the cyber realm are neither recognisably war nor peace but between these concepts, a situation of unpeace [3, p77].’

Appendices

Each of the three alternative ways of achieving the same effects – cyber, low and high intensity alternatives – have been ranked within the PESTLE framework based on which achieved the best and worst outcomes for the aggressor. This gives a way to compare attacks across the six categories considered: political, economic, socio/cultural, technological, legal and environmental.

- Final scores are an indicative measure of the greatest **return on effort for the attacker, for the cost incurred**. A higher score indicates the superior choice

These scores represent a qualitative assessment based on my own judgement and interpretation of the attacks, rather than a scientific analysis. My prior experiences working within the PwC Advisory practice provides me with the skills and knowledge required to apply business strategy frameworks to an area which is traditionally analysed more broadly through the lens of nuclear or military strategy.

To determine the overall score for each method initial values of 2 for best, 1 for medium and zero for the worst outcomes in each of the six categories will be assigned.

The six categories of PESTLE will themselves be weighted as the relative importance of political success (or failure) will, in general be higher than the environmental impact in the eyes of the attacker. The default rating used will be: political, economic, socio/cultural and legal having a default weighting of 3; technological a default weighting of 2; and environmental a default rating of 1.

This method allows the relative importance of each category to be taken into account, and whilst these will be held constant throughout the majority of the attacks, each of the ten case studies chosen will be reviewed on an individual basis to adjust levels if required.

The environmental scores have not been altered downwards even when there is little effect on the environment across the attacks, due to the ratings already taking this into account. For example, if all attacks are negligible on the environment, they will all be given a ‘best’ rating with a net neutral effect overall when the three attacks are being compared.

The detailed PESTLE analysis for each of the ten case studies are found within appendix 1-10. Each begins with a description of how the score was changed from the base level and why this change was made.

Appendix 1: Results for Estonia

Political weighting increased from 3 to 4 as the attack was about Russia asserting its political power over Estonia.

Socio/cultural weighting increased from 3 to 4 as the cultural significance of a Russian statue was behind the attacks with both sides relying on the nationalism of their populations, and social disturbance as a means of causing change to policy.

Legal weighting decreased from 3 to 2 because much of the attack was done through low level cyber weapons, distributed between many actors which meant prosecution was effectively impossible.

	Cyber weapon	Propaganda and street protests	Military show of force
Political	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Covert Plausible Deniability	Population unrest	Overt
	No loss of life	Local issue could spread nationwide	Threats through show of military power
	NATO agreement not triggered	Propaganda could shift from moving of a statue to politics	Damages soft power
	Retaliation limited	Hard to change top political actors	
	Estonian cyber defences increased		
Economic	Rating: Worst Score: 0	Rating: Best Score: 6	Rating: Medium Score: 3
	Co-ordinated attack, cost of staff and weapon development Useful as a training exercise for future cyberattacks	Estonia costs of cleaning up and policing protests/riots	Resources already present (fixed costs) and budget would exist for training exercises so negligible extra financial outlay
	Estonian government and businesses lost revenue	Protesters civilian population so unpaid	Cost to deploy air and land military resources
	Servers not damaged in DDoS attack so didn't need replacing	Propaganda costs relatively low	No financial cost for Estonia
Socio/ cultural	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Affected the majority of the population in their day to day life, with	Propagation targets nationalistic fever in Russian population	Cause distrust of Russia by Estonia
	Estonians very reliant on IT	Impact on population close to protests	Anxiety and distress from threat
	Increase in patriotism from population on both sides		
Technological	Rating: Worst Score: 0	Rating: Best Score: 4	Rating: Medium Score: 2

	Hackers noted to be sophisticated, able to adapt to defence	Propaganda very old form of disseminating specific message	Pre-existing forces
Legal	Rating: Medium Score: 2	Rating: Worst Score: 0	Rating: Best Score: 4
	Not really any physical damage with no direct loss of life	Protestors turning violent can be arrested and charged for a criminal offence	Russia is using its legal rights to redeploy forces and parade its military in its own borders
	Creation of the Tallinn Manual	No specific legal framework for propaganda	
	Plausible deniability		
Enviro-mental	Rating: Medium Score: 1	Rating: Medium Score: 1	Rating: Worst Score: 0
	Servers blocked for a period of time rather than broken so didn't need replacing	Damage caused by protesters needed to be disposed of and replaced	Redeployment of troops and equipment plus flypasts requires petrol/diesel
			Causes an increased air pollution

Table 18: PESTLE analysis for Estonia

Appendix 2: Results for Georgia

Political weighting increased from 3 to 4 as the attacks were used to support Russia's military invasion of Georgia.

Socio/cultural weighting increased from 3 to 4 as the aim of the attack was to prevent news spreading to other countries, as well as internally allowing Russia to control the narrative and prevent Georgia from publicising its view of events.

	Cyber weapon	Cut communications channels	More military forces and equipment
Political	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Covert	Hard to cut all channels so some news could get out	Communication hubs near dense populations so risk of casualties
	Plausible deniability - still no proof Russia behind the attack	Difficult to retain control mid-term	Higher kinetic strike risks retaliation and/or other countries assistance

	No loss of life from cyber element	Some evidence often left in sabotage / espionage operations for attribution	Damaged networks impacts ability to control the local narrative once in charge
	Population not highly reliant on IT - only 7% use internet	Capture risk of agents creates potential source of embarrassment or political retribution	Escalation of effect
	Buys time for Russia to sculpt narrative		
Economic	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	Training of hackers needed to take out the targets	Team recruited to destroy / sabotage infrastructure requires funding	Attack already under way so incremental cost of further strikes
	Georgia costs to restore functioning of its IT systems	Reconnaissance to find weakness	Heavy damage to Georgia through expensive equipment being destroyed and needing replacement
		Modelling ensure all comms channels hit	
Socio/ cultural	Rating: Medium Score: 4	Rating: Best Score: 8	Rating: Worst Score: 0
	Population not highly connected to the internet	Similar to cyberattack in that is it not a highly connected society	Communication hubs with workers near homes could result in civilian casulties
	Attack mainly commercial and governmental sites	Affects maybe felt later with population realising vulnerability	Anxiety and psychological distress given country being bombed
	Prevented news flow to other societies in order to tilt the narrative to Russia's favour		Hard to return to pre-invasion norms (communications down)
Technological	Rating: Worst Score: 0	Rating: Best Score: 4	Rating: Medium Score: 2
	Cyberattack was highly coordinated and timed.	Mainly small weapons or explosives to enter and destroy communications	Pre-existing weapons

Legal	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	Plausible deniability places it on the edge of attribution and legal repercussions	Small teams with less destruction of kinetic attack	Under the rules of war requires imminent danger to the acting party to proceed
	Deliberately opaque, still no full attribution	Physical destruction may constitute act of war (but already at war)	Attributable to Russia if done kinetically
	Use of cyber militia	Still in war imminent danger criteria needed	
Environmental	Rating: Best Score: 2	Rating: Medium Score: 1	Rating: Worst Score: 0
	No damage	Destruction of equipment	Loss of human life possible
	Temporary DDoS or defacement attacks	More destructive than cyber	Disposal of damaged buildings and devices
	Virtual not physical effects	Less destructive than missile strike	Rebuild materials

Table 19: PESTLE analysis for Georgia

Appendix 3: Results for Stuxnet

Political weighting increased from 3 to 4 given the cyberattack entered into due to political negotiations over Iran's enrichment of uranium.

Technological weighting increased from 2 to 3 due to the fact Stuxnet was the most technical piece of malware ever been produced with multiple zero days.

Environmental weighting increased from 1 to 2 because targeting of a nuclear power plant has the potential to cause nuclear contamination if operations affected.

	Cyber weapon	Special ops team	Missile strike
Political	Rating: Best Score: 8	Rating: Worst Score: 0	Rating: Medium Score: 4
	Covert	If successful neutral to positive politically	Potential act of war
	Minimal loss of life – retaliation / escalation limited	Failure cost potentially catastrophic (captured team – hostage situation, propaganda material etc)	Strikes against sovereign targets tend to require government knowledge / approval – requiring cross party support and potential burning of internal political capital

	Plausible deniability		Hard to deny / contain
	Not aggressive, so no internal political fallout		
Economic	Rating: Worst Score: 0	Rating: Best Score: 6	Rating: Medium Score: 3
	Internal: High cost of development, mainly technical staff and testing for a solution which can be deployed covertly once	Target: Impact limited within the site, but wider than just the centrifuges; would stall redevelopment;	Internal: deployment of air and sea resources and the cost of ordnance would exceed that of the covert deployment team
	Delayed development of Iranian centrifuges, didn't kill the program	Attacker: cost of training and equipping special ops forces is high over their lifetime	If the strikes created retaliatory action, escalation of force deployment within the area would be very costly
	Target: Impact limited to primary site, centrifuges only allowing recovery over short term;		Target: Significant damage to the site and lengthy rebuild time and high costs (more so as limited providers of materials)
	Cost to protect against second strike is relatively low		
Socio/ cultural	Rating: Best Score: 6	Rating: Worst Score: 0	Rating: Medium Score: 3
	Low impact – majority of population unaware (if ever); buys time for political environment to mature	If successful providers the attacker with strong narrative of being able to infiltrate base and exit	Disruptive depending upon level of escalation
	Divisive opinions on extending capabilities and spying	Defending party seen to be weak within their borders, which impacts the ability of leaders to maintain aura of supreme power – failure costs seen as catastrophic	Potential sanctions and economic volatility
Technological	Rating: Worst Score: 0	Rating: Medium Score: 3	Rating: Best Score: 6

	Cutting edge – combination of multiple exploits / zero days; bespoke development	Limited – small arms	Pre-existing but advanced – laser guided system (ASM / SSM)
Legal	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	Covert	Small team with less destruction of kinetic attack.	Under the rules of war requires imminent danger to the acting party to proceed
	Deliberately opaque giving plausible deniability	Still need imminent danger criteria under rules of war	
	Specialised nature places it on the edge of attribution and legal repercussions	Attack within sovereign territory would be criminal	
Environmental	Rating: Best Score: 4	Rating: Medium Score: 2	Rating: Worst Score: 0
	Limited damage, risk of contamination of site with Uranium unlikely	Possible loss of human life and destruction of materials	High – contamination, loss of human life
		More destructive than cyber but less so than missile strike	Disposal of damaged building and rebuild materials

Table 20: PESTLE analysis for Stuxnet

Appendix 4: Results for Saudi Aramco

Economic weighting increased from 3 to 4 given the significant economic damage to Saudi Aramco with huge costs in lost contracts, business and replacement equipment.

Environmental weighting increased from 1 to 2 as the oil industry being targeted could impact the environment significantly if oil extraction and transportation affected.

	Cyber weapon	Target refineries	Target pipes and ports
Political	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	Appropriate retaliation for earlier attacks - energy sector attack on Iran	Assumed to be a covert act, if successful could be put down to industrial accidents / failure with limited political ramifications	Disruption of global oil distribution - through either pipelines or port blockades rapidly extends the influence of the attack to other nations
	Sought to demonstrate capabilities to US /	If approach failed, and team caught, significant political	Likely to generate support for victim within the international

	Israel as show of power; developing concept of mutual assured destruction in cyber	fallout as viewed as act of terrorism / aggression	community from those reliant upon it for oil such as the US
	By taking code from prior attacks and repointing to the new target sends warning that attacks will come back to you	Given importance of commodity, failed attacks will lead to sanctions and some physical retaliation	Will escalate to physical skirmishes and potential conflict
	Covert, plausible deniability		
Economic	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Required Aramco to repurchase huge quantities of hard drives and computer equipment	Cost of disruption - if successful - significant in terms of lost revenues and rebuilding costs	Port blockades and disruption requires large naval assets and / or ships to create blockades
	Disrupted billings and deliveries - product had to be given away for free in Saudi Arabia	Cost of action for aggressor relatively low - cost of training and deployment	Cost to build and deploy warships are upwards of £500 million; potential for large damage if escalates
	Cost to attacker would be lower as using elements of other weapons		Alternatively could be achieved cheaply through scuttling ships in the Suez Canal / Straits of Hormuz which would impact additional commodity routes
			Impact on target will be financially high due to loss of oil revenues: instability in supply could lead to volatility in oil prices, which have downstream impacts on commodities and manufacturing
Socio/ cultural	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	Destabilise oil supply creates disruption and panic	If successful and attributed to an accident, no major	Potential global impact as tensions rise (as per impounding of

		societal or cultural impacts	tanker carrying oil to Syria in Gibraltar)
	Long lasting duration of the effects without physical damage	If detected and attributed (or failed) will increase tensions worldwide	Will lead to sanctions and tensions within aggressor
	Changes way companies have to look at IT, security and the impact of attacks		
Technological	Rating: Worst Score: 0	Rating: Best Score: 4	Rating: Medium Score: 2
	Cyberattack was well planned and coordinated	Simple, uses existing technologies (people)	Utilises existing technology - albeit large and expensive units
Legal	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	Plausible deniability; distance limits repercussions, no extradition treaty exists	Attack within sovereign territory would be criminal	Disruption of international trade routes will lead to legal challenges
	Targeting specific company leads to a criminal act, not an act of war		Incursions in sovereign waters is an act of war
	Re-use of components of the original attack permits a defence / legitimate retaliation claim		
Environmental	Rating: Best Score: 4	Rating: Medium Score: 2	Rating: Worst Score: 0
	Lack of oil supplies could have reduced usage so positive for environment	Loss of human life possible	Loss of human life possible
	Diesel use from trucks wasted journeys to refill with oil	Damage to oil terminals will lead to significant environmental damage	Damage to oil terminals / pipelines will lead to significant environmental damage
		Rebuild materials	Damage could be spread over wide area

Table 21: PESTLE analysis for Saudi Aramco

Appendix 5: Results for F-35 IP theft

Political weighting increased from 3 to 4 given the IP for fighter jet used to build an equivalent fighter jet for China, which could be used for exerting power in the future.

Economic weighting increased from 3 to 4 as the US 'lost' two decades worth of research and development, with China not having to invest to obtain high level technology.

	Cyber option	Industrial espionage	Breaking into offices
Political	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Covert, may not be uncovered	More covert than break in but less than cyber	Overt, hard to deny
	Plausible deniability	Very long term play, no guarantee of document provenance	Major benefit of that theft going unnoticed is missing here
	Not aggressive, no loss of life	Affect trade relations	Criminal prosecution of intruders could be damaging politically
	Some reassurance documents are latest versions	If caught, criminal prosecution of spies could be damaging politically	Trade relationships damaged – sanctions unavoidable
	Limited retaliation - trade sanctions		
Economic	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	High cost of developing technical staff needed for highly secure system	Cost to find and train suitable insider or find a target in the company who could be manipulated	Cost to find and train team qualified
	US R&D expense extensive and obtained at lower cost	US research and development expense extensive and obtained at lower cost	Expensive equipment needed to penetrate highly secure area Intelligence gathering
		Intelligence gathering	Sanctions / trade war hard to avoid
Socio/ cultural	Rating: Worst Score: 0	Rating: Medium Score: 3	Rating: Best Score: 6
	Population may not know out about loss	Similar to cyber method if information successfully obtained	News of a physical break in would hit the population quickly

	News of loss took time to make public		Would be shock and anger valuable IP not being protected
	Could have longer term impacts if IP used against US		
Technological	Rating: Medium Score: 2	Rating: Best Score: 4	Rating: Worst Score: 0
	Combination of exploits which could need bespoke development	Less technological skills required	Pre-existing technologies
Legal	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	Plausible deniability	Various legal actions: Criminal charges Section 301 of the Trade Act	Various legal actions: Trade sanctions
	Various legal actions: Section 301 of the Trade Act	The Economic Espionage Act	Criminal charges
	The Economic Espionage Act	Trade sanctions	Section 301 of the Trade Act
Environmental	Rating: Best Score: 2	Rating: Best Score: 2	Rating: Medium Score: 1
	No damage noted	No damage	Minimal damage of building materials needing replacing

Table 22: PESTLE analysis for F-35 IP theft

Appendix 6: Results for Sony Pictures

Political weighting increased from 3 to 4 as actions resulted from a movie depicting the killing of the leader of North Korea, whose power relies on divine leadership.

Socio/cultural weighting increased from 3 to 4 with national fever raised in the US with people believing their freedom of speech was under threat from another nation.

Legal weighting decreased from 3 to 2 given the main aim was to disrupt the release of the film. Given the opponent was North Korea legal responses would be very difficult to enact.

	Cyberattack	Break into offices	Bomb cinema threat
Political	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Covert, plausible deniability	Criminal act by one country by another on sovereign territory	Act of terrorism, potential act of war if

			attributed to nation state
	Does not attack citizens, no imminent threat posed to life reduces escalation	Political blowback if evidence linking the break in to a nation state	Hard for plausible deniability
	Damages political relations between the two countries	Still a degree of plausible deniability if low level operation	More severe damage to global relations – even neutral countries would likely condemn
	Damages credibility and reputation of Sony Pictures	Still a degree of plausible deniability if low level operation	
Economic	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	With lower protection, cost of development of cyberweapons would be lower than attack on nation state or Stuxnet	Cost of team to break into Offices would be low, but as access to all of the material taken through cyber means would likely not be achieved	Whilst the lowest cost option would be treated as act of terrorism
	Impact on Sony: Sales impact on movies leaked during attack; flight of stars from future shows	Attribution of break in more complex so may not lead to sanctions	Damage to Sony limited to lost revenues from the film
	c.$35m to restore financial and IT systems [15]		Further economic sanctions – including from neutral countries – very expensive for little gain
Socio/ cultural	Rating: Best Score: 8	Rating: Worst Score: 0	Rating: Medium Score: 4
	Sony suffered massive reputational damage; dominated news cycle for weeks about the nature of free speech and American values	Likely fails to gain enough material to dominate the news cycles	Would achieve short term disruption on US moviegoers
	Reduced funding for other media coverage of North Korea for fear of reprisals	No kudos for North Korea	
	Negative impact of the attack increased awareness and viewings of the film		

Technological	Rating: Worst Score: 0	Rating: Medium Score: 2	Rating: Best Score: 4
	Development of new capabilities	Simpler attack vector (physical break in easier way of navigating firewalls and security)	No new technology required
Legal	Rating: Best Score: 4	Rating: Medium Score: 2	Rating: Worst Score: 0
	No fallout for N Korea, disclosures lead to more legal repercussions for the victim than the aggressor	Criminal acts perpetrated within a different country	Likely act of war if attributed to nation state
Environmental	Rating: Best Score: 2	Rating: Best Score: 2	Rating: Best Score: 2
	No damage noted	Limited impact	Limited (no actual explosions)

Table 23: PESTLE analysis for Sony Pictures

Appendix 7: Results for SWIFT

Political weighting decreased from 3 to 2 given the motivations were economic not political.

Economic weighting increased from 3 to 4 as the main motivation behind the attack was to extract money from the SWIFT transaction system.

Socio/cultural weighting decreased from 3 to 2 given affects were mainly felt at the corporate level with everyday citizens not really hearing or being affected by the attack in their day to day lives.

Legal weighting increased from 3 to 4 because this was an act of theft which can be pursued through normal legal channels if the perpetrators are identified and apprehended.

	Cyberattack	Insider trading	Economic acts
Political	Rating: Medium Score: 2	Rating: Best Score: 3	Rating: Worst Score: 0
	Limited political benefit for attackers, allowed them to be portrayed as thieves from a failed state	Limited political benefit for attackers	Creating and deploying counterfeit currency is an act of economic war
	Highlighted risks and instabilities in	If captured, and monies traced would allow them to be	Permits aggressor to be painted as a rogue state

	systems, but not a major impact	depicted as thieves from a failed state	
	President Obama argued the US should pledge never to attack or interfere with financial markets, given the tremendous negative impact it could have in the global economic system		Overall political impact on the victim limited unless volumes so high as to devalue currency
			Expected to lead to sanctions
Economic	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Provided almost $2 billion in revenues to North Korea, slowly bled out of the financial systems over time	Would likely not produce as high a revenue stream as a cyberattack - would require insider information on multiple companies, plus capital to secure options / short sell	Does not generate significant income for aggressor - hard to drop billions into financial systems easily
	Losses spread over multiple parties - no one bank particularly badly hit	Greater traceability of financial positions leads to earlier detection and paper trails	Requires costly printing machines and plates to develop suitable forgeries for mass deception
	Cost of sanctions applied to North Korea will have been high		
Socio/ cultural	Rating: Best Score: 4	Rating: Worst Score: 0	Rating: Medium Score: 2
	No major impacts to target countries and companies	Optics will present aggressor as a thief reducing standing on the world stage	Unless very large scale unlikely to cause significant disruption within the victim
	Highlighted vulnerabilities within the security of the banking industry leading to investment and change	Doesn't bring any new capabilities or threats to the aggressors arsenal, so no increase in kudos for them	Tangible nature of the act (vs. insider trading) provides props for internal use to allow continued depiction of leaders as strong

Technological	Rating: Worst Score: 0	Rating: Best Score: 4	Rating: Medium Score: 2
	Multiple exploits and weaknesses required	No new attack vectors required	Requires advanced counterfeiting toolkit
Legal	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Theft	Criminal acts perpetrated within a different country	Will lead to legal sanctions given nature of counterfeiting
	Prosecution of some individuals sought	Prosecution of some individuals sought	
		Insider trading carries higher financial penalties than theft	
Environmental	Rating: Best Score: 2	Rating: Best Score: 2	Rating: Best Score: 2
	No major impact with damage reversible	No major impact with damage reversible	No major impact with damage reversible

Table 24: PESTLE analysis for SWIFT

Appendix 8: Results for Ukraine power

Political weighting increased from 3 to 4 as the motivation for the attack was to assert Russian dominance over the Ukraine and to show power.

Socio/cultural weighting increased from 3 to 4 with affects felt by the population losing power plus anxiety and fear over their nation not being able to prevent this attack.

	Cyberattack	Turn off gas supply	Transformer damage
Political	Rating: Best Score: 8	Rating: Worst Score: 0	Rating: Medium Score: 4
	Attacks sent shockwaves through the political sphere increasing focus upon cybersecurity and defence needs	Switching off supply impacts many more countries than Ukraine - Southern Mediterranean Countries impacted more as Ukraine has increased storage capacity to cope with this	Physical attacks on Government property is an act of terrorism or war
	Unlike prior attacks on Ukraine power networks - shutting off gas in pipelines - this only hit the	Spreads the impact of the attacks elsewhere - leading to increased political pressure on aggressor	Given nature of disruption - taking down nation infrastructure would potentially lead to NATO involvement,

	Ukraine, limiting the political fallout		escalating the situation
	Demonstration of show of force and the ability to damage energy supplies	Overt political act from the 'intimidate Ukraine playbook' - easy to spin bullying narrative by aggressor	Sanctions expected from Ukraine Allies
	Overt, physical impacts		
	Difficult to deny given target, history		
Economic	Rating: Worst Score: 0	Rating: Medium Score: 3	Rating: Best Score: 6
	Required two simultaneous attacks - one basic a basic DDoS on the phone lines and one designed for specific targets	Longer term movement towards development of new supply sources to reduce dependency on Russian gas creates longer term challenges to aggressor	Significant disruption to Ukraine economy as transformers take time to source; in the interim manufacturing, heavy industry would be limited to balance power distribution
	Caused widespread disruption to homes and businesses for limited period	For Ukrainian firms potential short term spikes in energy costs as supplies slow	Sanctions may be costly, but none were enacted on prior disputes suggesting would not be used
	Only electricity disrupted	Gas revenues for aggressor nation would drop in the short term	Low cost to aggressor - targets neither strongly fortified or secured
Socio /cultural	Rating: Best Score: 8	Rating: Worst Score: 0	Rating: Medium Score: 4
	With increased gas storage to counter pipeline closures, this would demonstrate still under the risk of Russian influence	With such events happening multiple times before - and the inability to permanently shut down supply - citizens will see this as just another attempt to intimidate	Black outs, coupled with dark winter nights creates powerful fear in the population
	Black outs, coupled with dark winter nights creates powerful fear in the population	For aggressor implies limited playbook, and predictability is easier to defend and makes them look	Maintains 'fear' of Russia in citizens minds, influencing elections and policies

		unimaginative and weak	
	Combination of two attacks increased fear and confusion		
Technological	Rating: Medium Score: 2	Rating: Best Score: 4	Rating: Medium Score: 2
	Basic attacks - DDoS - easily developed	No new skills required	No new skills required, but munitions, strike force needed
Legal	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	Despite NATO sending aid stopped short of declaring sanctions against Russia	Risks violating international supply contracts beyond the Ukraine	Likely act of war if attributed to nation state
	No legal ramifications		
Environmental	Rating: Best Score: 2	Rating: Best Score: 2	Rating: Best Score: 2
	Limited damage	No major impact - reversible	No major impact - reversible

Table 25: PESTLE analysis for Ukraine power

Appendix 9: Results for US election

Political weighting increased from 3 to 4 given there was a highly political motivation, influencing campaign during election of the next US President.

Economic weighting decreased from 3 to 2 given the political motivation and impact rather than financial.

Socio/cultural weighting increased from 3 to 4 with shocks over the ability of one nation state to affect the democratic process of another nation state. News cycles amplifying the Russian narrative to the population through home grown media.

	Cyberattack	Traditional propaganda	Start a war
Political	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Lead to impeachment proceedings and increasing the partisan nature of US politics	Will fuel unrest and political division intra and inter-party; limiting the functionality of governments	Requires the identification of a potential conflict / cause which politicians will rally around

	Fuelled unrest and political division intra and inter-party; limiting the functionality of governments	Short term impacts - but once channels open and working can have a longer term impact	High risk politically - intention to place country on alert to migrate the political narrative
	Created not just a short term challenge, but dominated the political landscape for years.	As sources more overt easier to deal with for the defender	
	Covert, plausible deniability	Plausible deniability	
Economic	Rating: Best Score: 4	Rating: Medium Score: 2	Rating: Worst Score: 0
	Impacts on US hard to quantify, but far reaching over a long time period	Cost to attacker higher as requires ownership of editorial TV networks	Requires troop movements, appropriation of funds
	Lost sessions of government will not be recovered	Impacts on US hard to quantify, but far reaching over a long time period	Potentially very high cost if conflict arises
	Cost to attacker low		
Socio/ cultural	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0
	Helped fuel division within US politics	Would fuel division within US politics	Will create a culture of fear / apprehension within both states
	Microtargeting of campaigns limited right to reply and allowed ideas to propagate	Broader targeting and broadcast distribution increases ability of the target to identify and reply to the propaganda	If intent is for short term crisis to move the political landscape, initial aggressor will likely have to back down, showing weakness
	Increased awareness of dangers of big data mining		
Technological	Rating: Medium Score: 2	Rating: Best Score: 4	Rating: Best Score: 4
	Piggybacked upon existing machine learning techniques	No new technology required	No new technology required
Legal	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0

	Lead to Impeachment of President of the United States	Higher traceability leads to increased likelihood of breaking an election campaign rule	Act of war
	Numerous individuals found guilty of crimes - but predominantly related to obstruction of justice as opposed to an election related crime	Potential to have broadcast licence revoked, closing off path to market	
	Many of the techniques used were legal, but are not being subject to greater oversight and regulation		
Environmental	Rating: Medium Score: 1	Rating: Best Score: 2	Rating: Worst Score: 0
	Trump pulling out of Paris climate agreement	Impact from printed media	Pollution from equipment mobilisation
	Impact hard to quantify as uncertain alternative candidates policies		If war breaks out high impact on environment

Table 26: PESTLE analysis for election interference

Appendix 10: Results for WannaCry

Political weighting decreased from 3 to 2 because the attack was not politically motivated, motives were more economic and to be disruptive.

Economic weighting increased from 3 to 4 with the initial purpose of the attack was to make money from ransomware.

Socio/cultural weighting increased from 3 to 4 with significant impact on the UK population, with individuals unable to attend medical appointments and news covered on mainstream media spreading through the population.

	Cyberattack	Records doubt	Destroy data centre
Political	Rating: Best Score: 4	Rating: Worst Score: 0	Rating: Medium Score: 2
	Re-use of US Govt exploits will have placed hidden pressure on other governments to be	Creating doubt within government records is, for some areas such as health, equivalent to deletion	Physical attacks on Government property is an act of terrorism or war

	more responsible with cyber tools		
	Difficult to attribute to any nation state	Such an attack would create significant destabilisation of the government in power	However, compared to falsifying records would be of lower impact
	Created political problems within the attacked country as NHS taken down	With respect to medical records, could be seen as a cyber WMD as treatments would be halted and lives lost	Would lead to kinetic retaliation and sanctions
	Debate focussed more upon the lack of infrastructure and maintenance which caused the attack, than the intentions of the attacker	Likely to lead to sanctions for the attacking country and them being further exiled from the international stage	Targeting of civilian assets outside of rules of engagement in war
	Overt - mass disruption		
Economic	Rating: Medium Score: 4	Rating: Worst Score: 0	Rating: Best Score: 8
	Aims of delivering funds from ransomware not met - not all paid	Multi-stage attacks required to access and randomly change records	Relatively low costs of single attack - no infiltration required
	Short term operational cost of lost operating slots, increased cost of manual record keeping	Unlikely to be reversible, hence would not lead to ransom from those attacked	For victim, significant cost of re-digitisation of historic records, data audits to source systems to recover / validate correct entries; rebuild of new data centre
	£92m recovery cost low in terms of NHS capital budget (£5bn) or operating budget (£123bn)	For victim, significant cost of re-digitisation of historic records, data audits to source systems to recover / validate correct entries	Increased costs of testing - 12-18 months to recover
		Increased costs of testing - 12-18 months to recover	
Socio/ cultural	Rating: Best Score: 8	Rating: Medium Score: 4	Rating: Worst Score: 0

	Dominated the news cycles	Creates distress and confusion for large swathes of the attacked society	Creates distress and confusion for large swathes of the attacked society based upon the extent of records destroyed
	Target very close to most of society - impact more greatly felt as all touched by the NHS	As records relate to health likely to have a higher impact than other areas	Places attacked country on high alert of potential attacks
Technological	Rating: Best Score: 4	Rating: Worst Score: 0	Rating: Best Score: 4
	Utilised combination of exploits taken from nation states (reducing own development costs) and out of date systems	Would likely be a complex attack to edit / alter historic records	Simple, known technologies
Legal	Rating: Best Score: 6	Rating: Medium Score: 3	Rating: Worst Score: 0
	No major legal ramifications	If attacker identified multiple angles for legal challenges and lawsuits	Potential act of war, minimum act of terrorism
Environmental	Rating: Best Score: 2	Rating: Medium Score: 1	Rating: Worst Score: 0
	Limited damage	Increased medical equipment needed to re-test patients	Loss of human life possible
			Disposal of damaged buildings and devices
			Rebuild materials

Table 27: PESTLE analysis for WannaCry

Acronyms

APT	Advanced Persistent Threat
DDoS	Distributed Denial of Service
IoT	Internet of Things
IP	Intellectual Property
IT	Information Technology
NATO	North Atlantic Treaty Organisation
NHS	National Health Service
NSA	National Security Agency
PESTLE	Political, Economic, Social, Technological, Legal, Environmental analysis framework
SWIFT	The Society for Worldwide Interbank Financial Telecommunication
SWOT	Strengths, Weaknesses, Opportunities, Threats
UN	United Nations
US	United States
WMD	Weapon of Mass Destruction

References

[1] J. Kallberg, "Strategic Cyberwar Threory - A Foundation for Designing Decisive Strategic Cyber Operations," ResearchGate [Online], October 2015. Available: https://cyber.army.mil/Portals/3/Documents/publications/external/Strategic%20Cyberwar%20Theory.pdf

[2] Inkwood Research. Global Cyber Weapons Market Forcast 2018-2026, 2008.

[3] L. Kello, The Virtual Weapon and International Order, Hampshire: Yale University Press, 2018.

[4] R. Sawyer and M Sawyer, The Art of War, Boulder: Westview, 1994.

[5] L. Seebeck, "Why the fifth domain is different," The Strategist [Online], Sep 5 2019. Available: https://www.aspistrategist.org.au/why-the-fifth-domain-is-different/

[6] M. Rogers, Testimony on US Cyber Command before the Senate Armed Services Committee, [Online], May 9 2017. Available: https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

[7] P. Paganini (2016, June. 18). NATO officially recognized cyberspace a warfare domain [Online]. Available: https://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html

[8] T. Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies, vol. 35, pp 5-32, 2012.

[9] J. Stone, "Cyber War Will Take Place," Journal of Strategic Studies, vol. 36, pp. 101-108, 2013.

[10] "I. Lachow and T. Grossman, ""'Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations,"" in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp.384-385."

[11] Fandom. (2009). Modern Day Military Pricing List [online]. Available: https://nation-creation.fandom.com/wiki/Modern_Day_Military_Pricing_List#:~:text=%20%20%201%20Hyuga%20CVH%20%28offically%20DDH%29%3A,Osumi%20LPH%20%28officially%20LST%29%3A%20~%24250-300%20million%20More%20#:~:text=%20%20%201%20Hyuga%20CVH%20%28offically%20DDH%29%3A,Osumi%20LPH%20%28officially%20LST%29%3A%20~%24250-300%20million%20More%20

[12] "S. Bellovin, S. Landau and H. Lin, ""Limiting the Undesired Impact of Cyber Weapons: Technical Requirements

and Policy Implications,"" in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp. 267"

[13] D. Kilcullen, The Dragons and the Snakes. How the rest learned to fight the west, London: C. Hurst & Co., 2020, pp. 162.

[14] Q. Liang and W. Xiangsui, Unrestricted Warfare, Beijing: PLA Literature and Arts Publishing House, 1999

[15] B. Buchanan, The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics, Cambridge: Harvard University Press, 2020.

[16] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired [Online], Aug. 22 2018. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[17] M. Hypponen, "Keynote: The Next Arms Race," Black Hat Asia 2019 [Online], 2019. Available: https://www.youtube.com/watch?v=l2rIVdpMToM

[18] "J. Mallory, ""Straw man architecture for International data exchange and collaborative analysis,"" MIT [Online], July 8 2011. Available: http://www.syssec-project.eu/m/page-media/23/bic2011-06-mallery.pdf"

[19] A. De Moraes, "MN2205 STRATEGIC MANAGEMENT," Royal Holloway University of London, 2019/20.

[20] M. Carr, US power and the internet in international relations the irony of the information age, Basingstoke: Palgrave Macmillan, 2016.

[21] C. Cope, Warfare in the fifth domain: A realistic threat or hyperbole, Royal Holloway University of London, 2017.

[22] M. Smeets, "How Much Does a Cyber Weapon Cost? Nobody Knows" [online] Nov 21 2016. Available: https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows

[23] T. Grugg, "A short course in cyber warfare," Black Hat Asia [Online], 2018. Available: https://www.youtube.com/watch?v=gvS4efEakpY

[24] HM Government, (2016), "National Cyber Security Strategy 2016-2021," [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[25] L. Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," International Security, Vol. 38, pp. 7-40, 2013.

[26] P.W. Singer and A. Friedman,Cyberseecurity and cyberwar what everyone needs to know, Oxford: Oxford University Press, 2013.

[27] H. Lin and A. Zegart, "Introduction," in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp. 7.

[28] J. William, (Sep/Oct 2010) "Defending a New Domain," Foreign Affairs [Online]. vol. 89, issue 5. Available: http://web.b.ebscohost.com.ezproxy01.rhul.ac.uk/ehost/detail/detail?vid=1&sid=17529d05-e73d-4b7e-a078-436475cc1a5f%40pdc-v-sessmgr01&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=52957873&db=bth

[29] M. Hayden, Playing to the Edge: American Intelligence in the Age of Terror, New York: Penguin, 2017, pp. 147.

[30] M. P.Fischerkeller and R. J.Harknett. (2017). "Deterrence is Not a Credible Strategy for Cyberspace." Orbis [Online]. Vol. 61, issue 3, pp. 381-393. Available: https://www.sciencedirect.com/science/article/abs/pii/S0030438717300431

[31] S. Smith. (2018, Jan). "Introducing Feminism in International Relations Theory." E-International Relations [Online]. Available: https://www.e-ir.info/2018/01/04/feminism-in-international-relations-theory/

[32] L. Kello. (2014). "The Virtual Weapon: Dilemmas and Future Scenarios". Politique étrangère[Online]. vol. 79, issue 4. Available: https://www.cairn-int.info/article-E_PE_144_0139--cyber-arms-problems-and-possible.htm#

[33] N. Inkster, "Measuring Military Cyber Power," Global Politics and Strategy, vol. 59, pp. 27-34, July 2017.

[34] M. Burgess. (2017, Apr. 18). Hacking the hackers: everything you need to know about Shadow Brokers' attack on the NSA [Online]. Available://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers

[35] B. Schneier, "Attack Attribution in Cyberspace," in Schneier on Security: We Have Root, B. Schneier, Indiana: John Wiley & Sons, 2019.

[36] H. Farrell and C. L. Glaser, ""How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine,"" in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp.58."

[37] L. H. Newman. (2019, June. 23). Iran shot down one of the most advanced spy drones ever made [online] Available: https://www.wired.co.uk/article/rq-4a-global-hawk-drone-us-iran

[38] K. Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired [Online], July 11 2011. Available: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

[39] H. Farrell and C. L. Glaser, ""How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine,"" in Bytes, Bombs, and Spies: The

Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp.58."

[40] P. Paganini. (2018, Mar. 8). Leaked NSA dump contains tools developed by NSA Territorial Dispute to track state-sponsored hackers [Online]. Available: https://securityaffairs.co/wordpress/69987/intelligence/nsa-territorial-dispute.html "

[41] Inkwood Research. (2018, May). Global Cyber Weapons Market Forcast 2018-2026 [Online]. Available: https://www.marketresearch.com/Inkwood-Research-v4104/Global-Cyber-Weapon-Forecast-11702567/

[42] The Free Dictionary. (2014). Act of war [Online]. Available: https://www.thefreedictionary.com/act+of+war

[43] North Atlantic Treaty Organisation. (2019, Nov. 25). Collective defence - Article 5 [Online]. Available: https://www.nato.int/cps/en/natohq/topics_110496.htm

[44] "EU Cyber Direct. (2018, July 9). The application of existing international law in cyberspace: state practice and key concepts [Online]. Available: https://www.iss.europa.eu/sites/default/files/EUISSFiles/programme_international%20law%20in%20cyberspace_07.07.2018.pdf"

[45] Department of Defense, Office of General Counsel, “Weapons,” in Law of War Manual (2015), p. 340.

[46] M. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence. Tallinn manual on the international law applicable to cyber warfare : Prepared by the international group of experts at the invitation of the NATO Cooperative, New York : Cambridge University Press, 2013.

[47] M. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.

[48] M. L. Gross, D. Canetti and D. R. Vashdi, ""Its Effects on Psychological Well-Being, Public Confidence, and Political Attitudes,"" in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp. 239."

[49] G. M. Graff, Dawn of the Code War, PublicAffairs, 2018.

[50] Fandom. (2009). Modern Day Military Pricing List [online]. Available: https://nation creation.fandom.com/wiki/Modern_Day_Military_Pricing_List#:~:text=%20%20%201%20Hyuga%20CVH%20%28offically%20DDH%29%3A,Osumi%20LPH%20%28officially%20LST%29%3A%20~%24250-300%20million%20More%20#:~:text=%20%20%201%20Hyuga%20CVH%20%28offically%20DDH%29%3A,Osumi%20LPH%20%28officially%20LST%29%3A%20~%24250-300%20million%20More%20

[51] The Independent. (2009, Dec. 18). Iraqi insurgents hack US drones" [online]. Available: https://www.independent.co.uk/news/world/middle-east/iraqi-insurgents-hack-us-drones-1844556.html

[52] W. Ashford. (2018, May 11). WannaCry's EternalBlue exploit still a threat, [Online]. Available: https://www.computerweekly.com/news/252440964/WannaCrys-EternalBlue-exploit-still-a-threat

[53] Zerodium. (2019). Our Exploit Acquisition Program [Online]. Available: https://zerodium.com/program.html

[54] M. Hosenball. (2016, Apr. 29). FBI paid under $1 million to unlock San Bernardino iPhone [Online]. Available: https://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032

[55] J. Healey and B. Buchanan. (2019). The Risks and Opportunities of Employing Offensive Cyber Operations [Online]. Available: https://www.youtube.com/watch?v=Ez1XwksXuO8

[56] M. Hypponen. (2019). Responding to a Cyber Attack with Missiles [Online]. Available: https://www.conferencecast.tv/talk-20213-responding-to-a-cyber-attack-with-missiles

[57] "L. Ablon and A. Bogart, Zero Days, Thousands of Nights The Life and Times of Zero-Day Vulnerabilities and Their Exploits, California: the RAND Corporation, 2017 [Online]. Available: https://www.rand.org/pubs/research_reports/RR1751.html"

[58] B. Schneier, "Disclosing vs. Hoarding Vulnerabilities," in Schneier on Security: We Have Root, B. Schneier, Indiana: John Wiley & Sons, 2019.

[59] J. Davies, "Hackers Take Down the Most Wired Country in Europe" [Online], Aug 21 2017. Available: https://www.wired.com/2007/08/ff-estonia/

[60] D. McGuinness, "How a cyber attack transformed Estonia," BBC News [Online], April 24 2017. Available: https://www.bbc.co.uk/news/39655415

[61] G. Keizer, "Estonia blamed Russia for backing 2007 cyberattacks, says leaked cable," [Online], Dec 9 2010. Available: https://www.computerworld.com/article/2511704/estonia-blamed-russia-for-backing-2007-cyberattacks--says-leaked-cable.html

[62] J. Markoff, "Before the Gunfire Cyberattacks," The New York Times [Online], Aug. 13. Aug. 13)Available: https://www.nytimes.com/2008/08/13/technology/13cyber.html

[63] A. Gotsiridze, (2019, Aug. 9). The Cyber Dimension of the 2008 Russia-Georgia War [Online]. Available: https://www.gfsis.org/blog/view/970

[64] K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Random House, 2014.

[65] E. Kaspersky. (2011, Nov. 2). The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight [Online]. Available: https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/

[66] L. Kello, "Correspondence: A Cyber Disagreement," International Security, vol. 39, no. 2, 2014.

[67] B. Groom, "Ministers Warn on Threat from Cyber Attacks," The Financial Times, Sep. 4 2012.

[68] R. Sale. (2012, Oct. 19). Saudi Insider Likely Key to Aramco Cyber-Attack [Online]. Available: http://www.ipsnews.net/2012/10/saudi-insider-likely-key-to-aramco-cyber-attack/

[69] Info Security. (2014, May 8). Saudi Aramco Cyber Attacks a ‘wake-up call’, Says Former NSA Boss [Online]. Available: https://www.infosecurity-magazine.com/news/saudi-aramco-cyber-attacks-a-wake-up-call-says/

[70] C. Kubecka, "How to Implement IT Security after a Cyber Melt-down," YouTube, Aug 6 2015

[71] J. Pagliery, "The inside story of the biggest hack in history" [Online] Aug 5, 2015. Available: https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

[72] Futurity. (1018, Apr. 16). How Does China Steal U.S. Intellectual Property? [Online]. Available: https://www.futurity.org/intellectual-property-theft-china-1730942/

[73] J. Rogin, "NSA Chief:Cybercrime Constitutes the 'Greatest Transfer of Wealth in History'" Foreign Policy (July 9, 2012).

[74] A. Schwarzenberg. (2019, Oct. 30). Section 301 of the Trade Act of 1974 [Online]. Available: https://www.wita.org/atp-research/section-301-trade-act-1974/

[75] S. Sumer. (2018, Dec. 9). Parmesan cheese and Sunbucks Coffee [Online]. Available: https://www.econlib.org/parmesan-cheese-and-sunbucks-coffee/

[76] K. Osborn. (2020, May. 27). The Real Reason Why China's J-31 Stealth Fighter Looks Like the F-35 [Online]. Available: https://nationalinterest.org/blog/buzz/real-reason-why-chinas-j-31-stealth-fighter-looks-f-35-157916

[77] D.Majumdar, "America's F-35 Stealth Fighter vs. China's New J-31: Who Wins?" National Interest [Online], (September 25, 2015). Available: https://nationalinterest.org/blog/the-buzz/americas-f-35-stealth-fighter-vs-chinas-new-j-31-who-wins-13938

[78] "DPRK FM Spokesman Blasts US Moves to Hurt Dignity of Supreme Leadership of DPRK," Korean Central News Agency, June 25, 2014.

[79] B. Hatch. (2018). "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits." Journal of strategic security [Online]. Available: https://search-proquest-com.ezproxy01.rhul.ac.uk/docview/2205359428/A326C99F98E744F8PQ/5?accountid=11455

[80] The Washington Post. (2015, Jan. 15). Why the Sony hack drew an unprecedented U.S. response against North Korea [Online]. Available: https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html

[81] BBC News. (2014, Dec. 29). The Interview: A guide to the cyber attack on Hollywood [Online]. Available: https://www.bbc.co.uk/news/entertainment-arts-30512032

[82] T. Johnson. (2014, Dec. 14). John McCain Calls Sony Hack Attack 'A New Form of Warfare' [Online]. Available: https://variety.com/2014/biz/news/john-mccain-calls-sony-hack-attack-a-new-form-of-warfare-1201384749/#!

[83] FireEye. (2018, Oct. 5). North Korean hackers used Swift network to steal more than $100m [Online]. Available: https://www.finextra.com/newsarticle/32742/north-korean-hackers-used-swift-network-to-steal-more-than-100m---fireeye

[84] M. Nichola, "North Korea Took $2 Billion in cyberattacks to Fund Weapons Program: UN Report," Reuters, Aug 5, 2019.

[85] S. Quadir, "Bangladesh Bank Exposed to Hackers by Cheap Switches, No Firewall: Police," Reuters, April 21, 2016.

[86] A. Nakashima. (2012, Sept. 21). Iran blamed for cyberattack on US banks and companies [Online]. Available: https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

[87] B. Hope and S. Vaishampayan, "The Stock Market Bell Rings, Computers Fail, Wall Street Cringes" The New York Times, July 2015.

[88] J. Markoff and T. Shanker, "Halted '03 IRAQ Plan Illustrates U.S. Fear of Cyberwar Risk," New York Times, Aug. 1, 2019

[89] M. Hypponen, "Cyber Arms Race," Les Assises, 2018.

[90] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired [Online], Mar. 3 2016. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[91] L. Ablon. (2017, Dec.) Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulns and Their Exploints [Online]. Available: https://www.youtube.com/watch?v=8BMULyCiSK4

[92] M. Rees, On the Future: Prospects for Humanity, Princeton: Princeton University Press, 2018.

[93] A. Kramer. (2006, Jan. 2). Russia Cuts Off Gas to Ukraine in Cost Dispute [Online]. Available: https://www.nytimes.com/2006/01/02/world/europe/russia-cuts-off-gas-to-ukraine-in-cost-dispute.html

[94] Siemens. Power Transformers [Online]. Available: https://new.siemens.com/uk/en/products/energy/high-voltage/transformers/power-transformers.html

[95] T. L. Thomas, "Russia's Reflexive Control Theory and the Military," journal of Slavic Military Studies, vol 17, pp. 237-56, 2004.

[96] O. Gazis and S. Becket. (2020, Aug. 18). Senate Intelligence Committee releases final report on 2016 Russian interference [Online]. Available: https://www.cbsnews.com/news/senate-report-russian-interference-2016-us-election/

[97] D. Kilcullen, The Dragons and the Snakes. How the rest learned to fight the west, Glasgow: Bell & Bain, 2020.

[98] C. Inglis, "" Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace,"" in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp. 239.

[99] M. Field, "WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled," The Telegraph [Online], Oct 11 2018. Available: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

[100] O. Hughes, "WannaCry impact on NHS considerably larger than previously suggested," Digital Health [Online], Oct 27 2017. Available: https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/

[101] National Audit Office. (2017, Oct. 27). Investigation: WannaCry cyber attack and the NHS [Online]. Available: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

[102] C. McGoogan, "Highly likely' WannaCry cyber attack was linked to North Korea' [Online]. May 23 2017, Available: https://www.telegraph.co.uk/technology/2017/05/23/highly-likely-wannacry-cyber-attack-linked-north-korea/

[103] W. Ashford, "Most Android devices running outdated versions," Computer Weekly [Online], 2016, Jan. 19). Available: https://www.computerweekly.com/news/4500271242/Most-Android-devices-running-outdated-versions

[104] O. Solon, "Hacking group auctions 'cyber weapons' stolen from NSA," The Guardian [Online]. Aug 16 2016. Available: https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group

[105] B. Schneier, "Disclosing vs. Hoarding Vulnerabilities," in Schneier on Security: We Have Root, B. Schneier, Indiana: John Wiley & Sons, 2019.

[106] M. Libicki, (2017) "The Convergence of Information Warfare," Strategic Studies Quarterly [Online]. vol. 11, issue 1. Available: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf

[107] "J. Healey, ""The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities, "" in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018."

[108] W. J. Clinton. (2000) Defending America's Cyberspace: National Plan for Information Systems Protection, Washington DC: The White House.

[109] G. W. Bush. (2003) The National Strategy to Secure Cyberspace, Washington, DC: The White House.

[110] H. Farrell and C. L. Glaser, ""How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine,"" in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018, pp.58."

[111] E. Gartzke and J. R. Lindsay, "Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations," H. Lin and A. Zegart, Eds. Washington, D.C.: Brookings Institution Press, 2018.

[112] J. Barrasso, M. Fallin and V. Foxx, Irepublican Platform 2016 Icleverland, OH: Consolidated Solutions, 2016 pp. 53.

[113] F. Hanson, (2015, Oct. 22). "Waging (cyber)war in peacetime" [Online]. Available: https://www.brookings.edu/blog/up-front/2015/10/22/waging-cyberwar-in-peacetime/