History repeating itself: how the media frames reporting on cyber conflict

> *"Read the newspapers. Remember that information in the press is at best only 40 percent accurate, but though it may not give you useful facts, it conveys attitudes. The context in which a person is mentioned often tells you more about her than what is alleged or stated."*
>
> *William Johnson (2009, 181).*

In this paper we examine the role that the news media plays in the production and transmission of knowledge about cyber conflict. We consider how the media draw on and influence the academic and cybersecurity practitioner debate. From the literature on news media framing, we draw out different forms of framing. We also consider the way that some news stories can become touchpoints; key events that are referred to as examples in future coverage of the same topic. We analyse the coverage of three examples of cyber conflict in the online archive of a broadsheet UK newspaper. In doing so, we highlight the role of key individuals who act as translators between networks of journalists, academics, and practitioners. Finally we look at reporting on cyber conflict in the Russia-Ukraine war.

Part One

Literature review

Goffman (1974) described frames as cognitive schemata that enable perception. In the hands of communications and media scholars, the concept evolved to refer to framing as a conscious act of selection by journalists (Koenig n.d.; Pieri 2019; Pan and Kosicki 1993; Vliegenthart and van Zoonen 2011).

Kitzinger (2007, 137) argues that news media framing goes beyond concepts of agenda setting or bias, "focusing instead on the *nature* of that attention and the aspects that are highlighted as *salient*". Similarly, she argues that "[t]he notion of 'bias' suggests that there is an objective and factual way of reporting an issue 'correctly'**.** The notion of 'framing', by contrast, suggests that all accounts of reality are shaped in some way or another" (2007, 137).

Beyond this general view of framing as intrinsic to news media production, there are a variety of sub-types of framing. Altheide (1997) explores how the news media has deployed what he terms the "problem frame". This mechanism of production prioritises formatting and entertainment-led approaches for garnering audience engagement. It produces content which frames fear as "a dominant [and routine] discourse" (Altheide 1997, 650).

Bennett and Lawrence (1995, 25) explore the role of news icons, described as striking visual or textual images that "journalists employ [...] to symbolically recount stories about larger issues". The examples they cite are iconic images that were frontpage news for prolonged periods, such as the Rodney King video which played a key role in reporting on racial tensions.

Kitzinger (2000, 75) examines how key events can become 'media templates' that set a firm pattern for future coverage of similar issues, like a template in a word processor application**.** These key events "serve as rhetorical shorthand, helping journalists and audiences to make sense of fresh news stories" (2000, 69).

The distinction between these forms of framing is not hard and fast, there is often overlap between these theorisations. These frames are socially constructed and capable of change. Kitzinger notes that while media templates "often seem natural or inevitable, they are actually

created and maintained by source strategies, social power relations and journalistic/audience reception processes" (Kitzinger 2000, 62). Moreover, they can be "modified through the interaction between contemporaneous and retrospective reporting" (2000, 70).

Jarvis, Macdonald, and Whiting (2016, 618) analyse how news media representations often appeal to authoritative witnesses, either through reference to their professional standing or the attribution of particular properties. Similarly, Stevens (2020) provides an examination of how malware analysts contributed to public understanding of the Stuxnet malware. This act of translation is one that people perform at the interface between academia, security research, and journalism.

Beyond the media, theories of framing have been applied to cybersecurity and threat construction. Bendrath, Eriksson, and Giacomello (2007) use frame theory to examine the construction of threat politics in cybersecurity. Similarly, Dunn Cavelty (2008, 21) introduces "a framework for the analysis of threat frames … partly based on the Copenhagen school's securitization approach". Building on Dunn Cavelty's insights, Jarvis, Macdonald, and Whiting (2016, 619–20) explore how generic historical analogies are used to construct cybersecurity threats related to cyberterrorism. Lawson and Middleton (2019) examine the framing of cyber security threats, including in news media, through the 'cyber Pearl Harbor' analogy.

Methodology

This paper is not another analysis of Stuxnet or the Estonian cyber-attacks. Rather, it is about the way that these events were reported initially and how this coverage changed over time. We undertook an exploratory analysis of *The Guardian's* coverage of cyber conflict. We chose *The Guardian* as an example of a mainstream newspaper. The paper's website also had an archive of articles tagged as 'cyberwar', which provided a starting point but was not a complete collection of the paper's coverage[1].

We used Google to search *The Guardian's* website. We recognise that this method is limited by Google's functionality. Google does not perfectly collate all publications and selectively omits

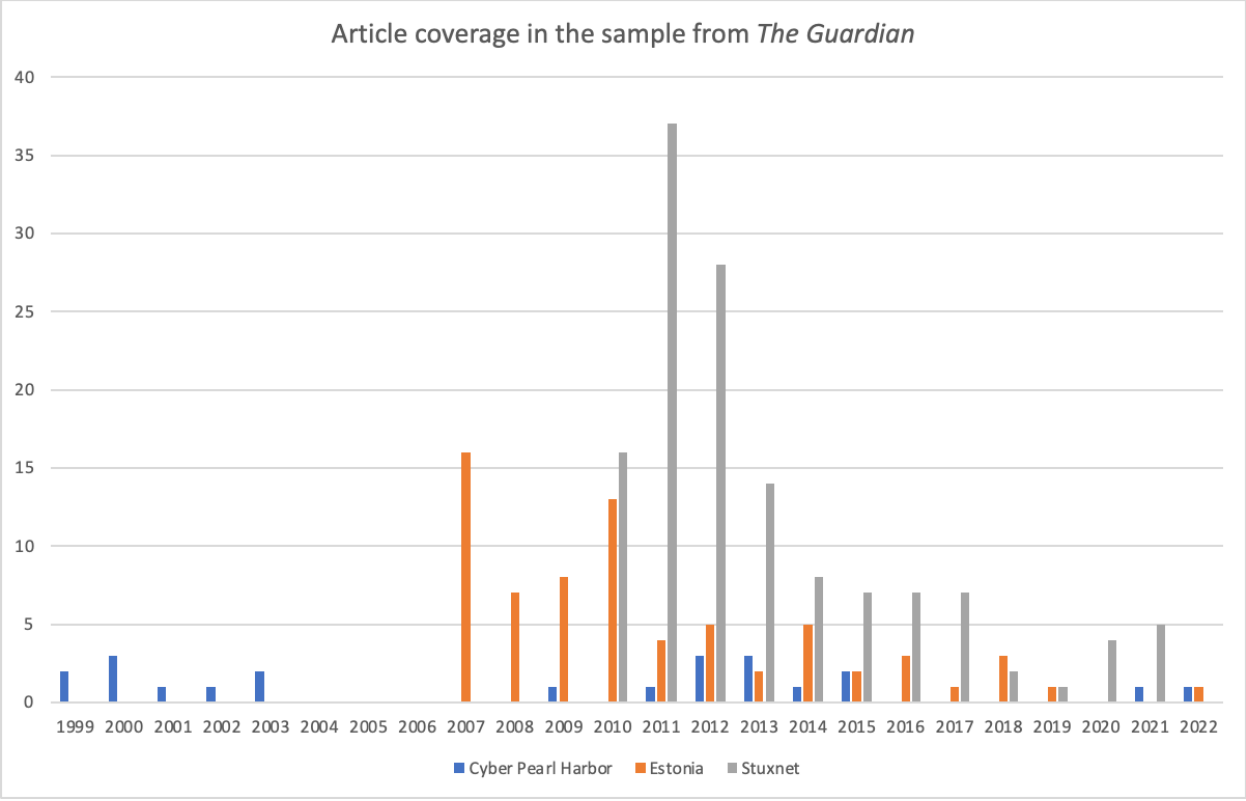
[1] https://www.theguardian.com/technology/cyberwar

entries deemed ‘very similar’ to results previously displayed. Example search terms can be seen below:

"electronic pearl harbor" site:https://www.theguardian.com/
"digital pearl harbor" site:https://www.theguardian.com/
"cyber pearl harbor" site:https://www.theguardian.com/
"stuxnet" site:https://www.theguardian.com/
"Estonia" "cyber" site:https://www.theguardian.com

The last query was intended to capture references to ‘Estonia’ that do not provide additional details about that case such as the year or the alleged aggressor – thereby capturing shorter references to these events. We then manually examined the results, discounting articles that did not mention the case in article text. This generated a set of 242 articles, which were stored in a shared online archive. Where articles were re-reporting claims originally published in other newspapers we also read those reports. *The New York Times* was a key source for *The Guardian* in this respect.

Figure 1. Article coverage in the sample from *The Guardian*



Coverage of cyber conflict was limited in *The Guardian* throughout the period. Most of the academic work cited in the literature review above was focused on the news coverage of high-profile events. For example, Kitzinger (2000) examines coverage of child abuse cases that became national scandals, prompting weeks of front-page coverage. In contrast, even at the peak of coverage of Stuxnet in 2011, it was still appearing in less than one article a week averaged across the year. Moreover, coverage of Estonia dropped after 2010, raising the possibility that Stuxnet moved Estonia down the news agenda.

We analysed these articles through the lens of the literature on news media framing examined above. Articles broadly fell into two categories: those about the episode in question or those where that episode was referenced in reporting on another event. In the second case we looked at how the original event was juxtaposed with other references and questioned what work the reference was doing for the article – asking why the journalist had included it in the piece. We created a chronology of articles referencing each case. This combined excerpts from the articles with our analytical commentary, including the identification of frames. We used these chronologies as the basis for the short descriptions of our findings set out below.

Part Two

Estonia 2007: the life of a news story

Our first case study concerns coverage of the series of cyber attacks that affected Estonia in 2007. This case illustrates the ways that events are framed throughout their life as a news story.

Normally at this point in an article we would provide a brief description of the event. This account would probably cite contemporary news or cybersecurity industry reporting, or longer journalistic accounts written after the events. Some parts of the event would be presented as factual. Others might be described as in need of revision. However, a key goal of this paper is to make visible the process by which exactly this kind of short summary account is created.

As such, the analysis below explores how the presentation of the events in Estonia changed over time. In the earliest coverage these attacks were framed as an extension of wider tensions with Russia. Over time, these events were cited more often as an example in articles about 'cyberwar'. Years later, the touchpoint of 'Estonia' was retrospectively re-framed in some coverage as an early example of hybrid warfare.

Initial framing – familiar political-diplomatic disputes

The early coverage underlines how unfamiliar cyber was for mainstream journalists in 2007. A feature article from 3 June 2007 refers to a "massive 'cyber-attack'", with single quotes suggesting the novelty of the term (Burke 2007). That is the only reference to cyber in the 2,400-word article – highlighting how limited the focus on cyber conflict was in *The Guardian's* reporting at the time.

The initial coverage appears in articles framed around the tension between Russia and the West. The first article in our sample to mention the attacks was written by Luke Harding and was headlined 'Protest by Kremlin as police quell riots in Estonia' (Harding 2007). This article focuses on acts of physical violence and their diplomatic repercussions, with the cyber attacks reported alongside acts of vandalism and looting. The cyber attacks are thus framed as something familiar for the reader; a digital version of physical unrest.

The diplomatic-political framing of the story affects the way that now-familiar aspects of cyber conflict are reported. For example, one report initially frames attribution not as a technical challenge but as a diplomatic one: “EU and Nato officials have been careful not to accuse the Russians directly” (Traynor 2007). Although the report then goes on to mention the debate about the technical challenges of attribution, these are given less prominence than the political aspects. Conversely, early reporting of Stuxnet (see below) tends to emphasise the technical challenges.

In some cases the attacks were explicitly framed using images from popular culture: “It reads like a John le Carre [sic] script. [...] Except the attack was a cyber-assault” (Sweney 2007). The comparison is made again in a book review in 2008 – “The events feel strikingly familiar, like updated versions of our favourite Le Carré novels” (Macqueen 2008).

Farivar (2009, 2–3) notes that the attacks on Estonia gained attention in a way that similar operations targeting Kyrgyzstan in 2009 did not. *The Guardian’s* report on that case highlights multiple competing possible explanations for the attacks (Bradbury 2009). However, that incident then dropped out of *The Guardian’s* coverage of cyber conflict; ‘Kyrgyzstan’ does not act as a touchpoint in the same way that ‘Estonia’ does. Explaining why is beyond the scope of this paper but it may be relevant that *The Guardian’s* reporting of Estonia used the familiar Cold War framing and the report on Kyrgyzstan did not.

Developing into a touchpoint and re-framing as early example of hybrid warfare

By 2008 references to the Estonian cyberattacks in *The Guardian* appeared primarily as examples of historical cyberattacks in articles about ‘cyberwar’ (Johnson 2008; Hinsliff 2008; Somaiya 2008). While these reports consider the Russia angle, the focus is on the mechanics of this phenomenon. ‘Estonia’ is cited alongside alleged cases of Chinese cyber-espionage, as an example of what is possible in this space (Johnson 2009).

Indeed after their initial newsworthiness, the events of 2007 in Estonia rapidly began to be summarised in one or at most two sentences in articles about other subjects. An article published on 4 September 2007 provides a typical example: “In May, the small Baltic country of Estonia was subjected to a three-week wave of hacking that disabled websites of government ministries, political parties, newspapers, banks and companies" (Tran 2007). Over time these

descriptions become simpler, as in a 2011 article that notes simply that: “In 2007, Estonia was almost cripped by a cyber-attack thought to originate in Russia” (MacAskill 2011b).

These ‘touchpoints’ are a product of the practicalities of news reporting. In the limited word count available, references to historical events are introduced for a specific purpose – for example, to support a claim or to provide balance. These touchpoints will usually be at most two sentences, and are frequently shorter. In online coverage, they will often include a hyperlink to earlier coverage of the article – a shortcut to nuance that is lost entirely in print coverage and which relies on the online reader to click through. Such short descriptions provide limited space for differing interpretations or nuance that might have been present in earlier reporting. As such, they encode a particular interpretation of what may initially have been reported as much more complex or uncertain events.

After the initial coverage of 2007, most of the references to these events in *The Guardian’s* coverage are of the short, touchpoint type. However, there are exceptions to this progression, with later, longer articles re-examining these events in retrospect (Kingsley 2012; Grassegger and Krogerus 2017).

One feature article from 2016 provides an example of ‘Estonia’ being reframed as an early case of “what has now become known as hybrid warfare” (Borger 2016). This came at a time, following Russia’s annexation of Crimea in 2014, when hybrid warfare was a high-profile phenomenon. A similar framing can be seen in a 2017 feature article with the standfirst: “The digital attack that brought Estonia to a standstill 10 years ago was the first shot in a cyberwar that has been raging between Moscow and the west ever since” (Grassegger and Krogerus 2017).

It is notable that these are both longer articles rather than news reporting. This is suggestive of the way that re-framing these events requires describing them in more detail, thereby allowing the aspects of the story most relevant to the new framing to be emphasised. The ‘meaning’ of events encoded in those touchpoints is not set, but can be changed through journalistic acts of re-interpretation.

Stuxnet: problem framing and the influence of key reports

The next case examines coverage of the Stuxnet worm. We again examine how Stuxnet went from being framed to becoming a touchpoint, and then highlight the contingency of this process.

From framings to touchpoints

In the Estonia case study, the first references to the cyber attacks appeared in reports framed around the broader political and military dispute with Russia. In contrast, the initial reporting of Stuxnet was framed as a novel computer security issue with a geopolitical component (Halliday 2010a; Meghani, Karimi, and Press 2010; Beaumont 2010b). Although these reports reference the Iranian nuclear programme, the focus of the story is on the new malware.

The contrast can be seen when the initial reports are compared to a series of articles by Julian Borger and Saeed Kamali Dehghan that are framed around the diplomatic and covert competition over Iran's nuclear programme (Borger and Dehghan 2010a; 2010b; 2011)**.** Stuxnet was in these accounts juxtaposed with diplomatic pressure, UN resolutions, and the assassination of Iranian nuclear scientists. These framings resembled the way that the Estonian cyber attacks were initially reported as a continuation of an existing dispute by new means.

These different framings shaped the way that the impact of the Stuxnet malware was reported. The early reporting on Stuxnet as a computer security issue focused on the novel or impressive aspects of the malware. Stuxnet was described as "above and beyond previous attacks of a similar nature", and "a very sophisticated attack" (Halliday 2010a). One article claimed that cybersecurity threats, "once a personal problem [...] could now be as daunting as a nuclear strike" (Naughton 2010b). In contrast, an article about the nuclear programme by Meir Javedanfar (2011) asserts that Stuxnet "did cause damage … [but was] not sufficient to stop Iran's nuclear programme in its tracks". Another asserted that "Stuxnet appears to have been, at most, a hiccup for Iran's nuclear ambitions" (Borger 2011).

As in the Estonia case, references to Stuxnet became condensed into touchpoint descriptions. Because of an influential *New York Times* article (see below), Stuxnet could be attributed with some caveats to the US, which allowed it to be used to introduce balance into reports on Russian or Chinese cyber activities. Sometimes these touchpoints are literally re-used between

articles. Articles about sabotage at the Natanz enrichment facility in 2020 and 2021 both used the same idiosyncratic description of Stuxnet – “the use of the Stuxnet computer virus, which scrambled code” – suggesting that the text was copied over from the previous article (Safi and Scammell 2020; Coulter 2021).

Early coverage of Stuxnet also established a recognisable template for coverage of subsequent malware discoveries. An article from 2011 on Symantec’s reporting of the Duqu malware provides an example of an article that displays elements of this template (Hopkins 2011b). The article’s headline is “‘New Stuxnet’ worm targets companies in Europe”. Within the article, Stuxnet is used as a touchpoint to explain the new malware, for example referring to the possible rise of “Stuxnet-style viruses”. More broadly, the article – in its structure, composition, its selection of sources, its tone – follows the template established by reporting about Stuxnet. Even the quote provided by the Symantec security researcher closely resembles the way that Stuxnet was described: “This is extremely sophisticated, this is cutting edge.” In this sense, Stuxnet functioned something like a news media template in Kitzinger’s sense; it created a pattern for reporting on the discovery of malware.

The contingent nature of common framings

The reporting on Stuxnet changed over time, with some details dropping out of the mainstream of reporting. In the case of Stuxnet, these include the claim that Stuxnet targeted the Bushehr nuclear reactor complex (Halliday 2010a; Halliday and Borger 2010; Beaumont 2010a; Halliday 2010b); that it was intended for espionage rather than sabotage (Beaumont 2010c); that it caused the failure of an Indian satellite (Naughton 2010a); that it was not the cause of the delay, which was due to performance issues with the Iranian centrifuges (Borger 2010; Borger and Dehghan 2010b; Halliday 2011); or that it could have caused “a new Chernobyl” (Arthur 2011).

None of these aspects of the story would likely be mentioned in a touchpoint-type description of Stuxnet written today. Viewing the early coverage with the benefit of hindsight can give the impression of the reporting gradually approximating the facts of the case. However, this impression is misleading. Our current understanding of this case is contingent and the widely accepted account of Stuxnet in mainstream journalism could have developed differently.

For example, in January 2011, then Russian ambassador to NATO Dmitry Rogozin said that the Stuxnet virus "could lead to a new Chernobyl". This claim was widely reported at the time (see for example Arthur 2011) but then dropped out of *The Guardian's* coverage. The accuracy of Rogozin's claim is largely beside the point – his comment provides a ready-made headline. Moreover, at the time, Stuxnet was often portrayed as potentially threatening to Western interests (Beaumont 2010b; Norton-Taylor 2010).

Similarly, the conviction of one person in an Estonian court in relation to a denial of service attack was widely reported in 2008, including in *The Guardian* (Arthur 2008). However, this event was not generally included in touchpoint-type descriptions in later coverage, with one exception (Borger 2014).

This case study also illustrates the influence that widely re-reported articles can have on the broader framing of an event in news coverage. In the case of Stuxnet, *The Guardian's* coverage was influenced by the publication on 15 January 2011 of an article in the *New York Times* 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay' (Broad, Markoff, and Sanger 2011). That article claimed that Israel's Dimona complex had been the site of testing for the Stuxnet worm, gave a history of the claimed joint US-Israeli operation behind the worm, and stated that Stuxnet had been an alternative to a conventional strike by Israel.

This report was based on access to well-placed sources and was the strongest allegation of responsibility to appear in mainstream media coverage at that time. There are reputational and legal risks for news outlets in making strong or novel claims (Ars Staff 2018). However, once published, other media organisations can then cite that report to make the same claim. *The Guardian's* report (MacAskill 2011a) adopted the *Times'* framing of Stuxnet as having delayed a conventional strike by Israel. *The Times'* reporting was widely cited in *The Guardian's* coverage, often being used as evidence that Stuxnet was created by the US or Israel. We suspect that the phenomena of specific articles becoming the most widely used source on particular claims will lead to the framing used in those articles becoming commonly used.

'Cyber Pearl Harbor': flexible framings and frame interaction

The third of our case studies considers ‘cyber Pearl Harbor’, exploring how analogy is used to represent threats in the absence of historical events. In the first part of this section we examine how this analogy has been repurposed to refer to different threats and in the second how the use of this analogy has changed as more cyber operations have become public.

Unlike the previous case studies, ‘cyber Pearl Harbor’ is an analogy to a historical incident rather than a news story in its own right. The term is a rhetorical shorthand for “cyber attacks against critical infrastructure leading to mass destruction and disruption” (Lawson and Middleton 2019). Implicit in the analogy is the idea that policymakers and officials “will fail to anticipate the scope, nature or target of a cyber attack and that the U.S. military or technological infrastructure will suffer catastrophic paralysis” (Wirtz 2017).

The analogy of ‘cyber Pearl Harbor’ communicates a complex issue in simple terms, providing what Goldman and Arquilla (2014, 5) term a “bridge between the familiar and the new”. Similar terms include ‘electronic 9/11’, ‘Clickskrieg’ and ‘cyber third world war’ (see for example (Hencke 2009; Sparrow 2010; Paul 2022a).

The flexible frame

‘Cyber Pearl Harbor’ has been a recurring theme in articles since 1999. Yet only one article in the sample used ‘cyber Pearl Harbor’ to frame a specific incident. This was a commentary by journalist Duncan Campbell claiming that a leak of the identities of 115 alleged UK intelligence officers constituted a “real electronic Pearl Harbor” in the UK (Campbell 1999). This framing amplifies the significance of this incident.

However, with the exception of Campbell’s (possibly ironic) use of the term, in our sample of articles, ‘cyber Pearl Harbor’ is not applied to events that have actually occurred, including any of the incidents of cyber conflict in the public record. Outside of our sample, we note that ‘cyber Pearl Harbor’ has been applied to events. See for example Ashton Carter’s description of the Snowden leaks as a ‘cyber Pearl Harbor’ (Belfer Center 2014).

The actor behind this imagined attack changes over time. In early articles the threat is the mythical teenage hacker in their bedroom (The Guardian 1999; Borger 2000). Post-9/11, the threat shifts to terrorism, with concerns around the teenage hacker becoming increasingly

peripheral (Ross 2003). In 2003, the focus is Iraq and its willingness to commit a “digital Pearl harbour”, though these concerns quickly became seen as non-existent (Rojas 2003). A cyberterrorist ‘cyber Pearl Harbor’ targeting Western economic infrastructure is consistently presented as an existential threat throughout this period, with some coverage going further to prominently highlight accounts that suggest such attacks could be used for fatal strikes on the public (Ross 2003).

Coverage from 2009 onwards becomes increasingly focused on state actors (Glenny 2009). This is a trend seen across coverage during this period, alongside a general downplaying of cyberterrorism concerns, though these still receive some mention (Hunker 2011; Greenwald 2013). These findings parallel those of Lawson and Middleton (2019), who note the changeable nature of the threat actor behind ‘cyber Pearl Harbor’ and how, over time, its focus becomes increasingly state-centric. While ‘cyber Pearl Harbor’ never occurs, it does change to meet the perceived threat of the moment.

Frame interaction and changing attitudes towards ‘cyber Pearl Harbor’

Over time, references to ‘cyber Pearl Harbor’ become increasingly critical, noting that it has not occurred and seems increasingly unlikely to do so (Glenny 2009; Carroll 2012)**.** These articles raise broader discussions around the nature of cyber conflict (Glenny 2009; Hunker 2011; Carroll 2012; Coviello 2013).

Misha Glenny’s (2009) article uses Estonia as a touchpoint, highlighting its role in prompting debate around offensive strategy. References to Estonia here draw attention to an emerging debate over cyber conflict and away from the disaster rhetoric of ‘cyber Pearl Harbor’.

Similarly, in an interview with John Arquilla, Rory Carroll (2012) highlights how Arquilla “did not fear a major ‘cyber-Pearl Harbor’ attack on the US” warning that “the risk was instead small, multiple attacks costing hundreds of billions of dollars.” Arquilla highlighted Stuxnet as an example of such a threat.

In some cases the analogy is strongly derided; for example Trevor Timm (2014) admonishes such terminology as “ridiculous fear-mongering catch-phrases”. Notably, these critiques at times draw on the academic literature; Timm’s critique links to an article in *The Washington Post*,

‘Cyber-Pearl Harbor is a myth’ (Farrell 2013), which is a synopsis of Eric Gartzke’s ‘The Myth of Cyberwar’ (Gartzke 2013). This example illustrates not only the feedback loops between different media sources, but also of the impact that academic perspectives can have in shaping media debate.

As part of this more critical approach, some articles examine how the concept of ‘cyber Pearl Harbor’ could be used as a pretext for greater government surveillance, a concern mostly absent in early coverage (with one exception, see Butcher 2002). Consequently, broader coverage emerges concerning fears around this surveillance state (Glenny 2009; Greenwald 2013; Timm 2014; Rushe and Ackerman 2015).

Between 2016 and 2020 we found no mentions of ‘cyber Pearl Harbor’ in our sample, a period encompassing major cyber incidents including Wannacry, NotPetya, and SolarWinds. One explanation may be that the term was not seen by journalists, or their sources, as capturing the dynamics of cyber conflict during this period. The frequency of references to ‘cyber Pearl Harbor’ in our sample broadly aligns with the findings of Lawson and Middleton (2019), with coverage peaking from the late 1990s into the early 2000s, declining around 2003 and increasing around 2011, though *The Guardian’s* coverage remained relatively consistent through to 2015 thereafter coverage dropped off again (unlike Lawson and Middleton who observed the peak from 2011 through to 2012).

Defining SolarWinds: discursive competition in action

The Guardian’s coverage of cyber conflict consistently relies on expert commentary. Key individuals and organisations were cited repeatedly, for instance Leon Panetta (Kiss 2012; Greenwald 2013; Bentley 2013; Rushe and Ackerman 2015) on ‘cyber Pearl Harbor’ or Symantec in early coverage of Stuxnet (Halliday 2010a; Meghani, Karimi, and Press 2010; Halliday 2010b; Hopkins 2011a; 2011b).

This is illustrative of the complex interconnection between academic, industry, and journalistic discourses on cyber issues. As Gamson and Modigliani note, “Journalists may draw their ideas and language from any or all of the other [public] forums, frequently paraphrasing or quoting their sources” (Gamson and Modigliani 1989, 3). Key figures act as translators between these

discourses, allowing the interchange of ideas but also at times prompting competition between alternative discursive formations.

An exchange between an academic and two journalists on Twitter in December 2020 provides an example of this dynamic. The exchange concerned reporting on the SolarWinds intrusion campaign and referred to the wider debate about how to characterise this activity. On 14 December, academic Thomas Rid tweeted a “subtle point on terminology [...] exfiltrating data … should not be called an ‘attack’” (Thomas Rid [@RidT] 2020).

Rid was retweeted by journalist Kim Zetter, who asked whether ‘infosec Twitter’ agreed with Rid’s characterisation (Kim Zetter [@KimZetter] 2020). This prompted vociferous debate. One of the respondents was journalist Nicole Perlroth, who tweeted that she disagreed with Rid, saying the espionage framing “downplays what we are currently witnessing” (Nicole Perlr🌻th [@nicoleperlroth] 2020). Most respondents to Zetter’s poll disagreed with Rid’s characterisation, prompting one commentator to tweet that this was “embarrassing” because it revealed that those people “likely don’t understand the differences between CNE and CNA”, using the US military’s terminology for these activities (Horkos 🌻 [@WylieNewmark] 2020). However, we view Perloth and Rid’s stances as reflecting competing but meaningful positions.

This exchange is an example of influential figures disputing the words that should be used in media coverage. The positions Rid and Perlroth advance are likely to have weight for journalists and sub-editors when they are writing or editing articles. As such, exchanges such as this one are part of a process of discursive competition that shapes contemporary reporting and which can lead to later re-framing of stories.

Part Three

Cyber conflict in the Russia-Ukraine War – early reporting

The Russia-Ukraine War has once again shown how far down the mainstream news agenda cyber is compared to kinetic conflict. As Rid noted in a *New York Times* opinion piece, “There’s no bigger story than the violent effects of war [...] In comparison, the sensationalist appeal of cyberattacks is significantly lower” (Rid 2022).

Reporting on the cyber aspects of the war therefore has to justify its existence given the much greater newsworthiness of the conventional aspects. Coverage of the cyber aspect of the Russia-Ukraine War has often therefore framed cyber as surprisingly absent or ineffective (Manjoo 2022; Martin 2022; Franceschi-Bicchierai 2022). This reporting is clearly connected to the academic and practitioner debate on this topic. Journalists cite experts from those communities and some articles are more about the debate than about the conflict itself (Manjoo 2022).

Coverage has walked a difficult line: reporting on known incidents but doing so while framing cyber as having been ineffective or absent. For example, on 1 April 2022 *The Guardian* ran an article with the headline ‘Russia’s slow cyberwar in Ukraine begins to escalate, experts say’ (Paul 2022b). According to that article, “Although Russia has been slow to carry out major attacks, it has been targeting Ukraine in other ways. On 24 February, more than 10,000 modems of the satellite broadband provider Viasat were knocked offline in a hack that US officials have attributed to Russia.” In this framing, the Viasat hack is reported but is not a ‘major attack’.

A similar balancing act is at work in a 9 March 2022 article in *The Guardian* (Paul 2022a) on the risk of an “unprecedented cyberwar” emerging from the Russia-Ukraine War. That article references Russian cyber operations but these are framed as distinct from the threatened ‘unprecedented cyberwar’. The article notes that “[experts] have warned for years of a ‘Cyber Pearl Harbor’”, with a hyperlink pointing to an opinion piece citing Panetta. The use of this term, and the similarly hyperbolic phrase “cyber third world war”, allows the author to point to a ‘catastophic’ cyber attack without having to describe what that would involve or explain how this would differ from the cyber operations referenced in the article.

Becoming a touchpoint and a template

In time the breadth and complexity of the current reporting on the cyber aspects of the Russia-Ukraine War will likely become simplified and condensed into a touchpoint that encodes a particular meaning. In this way, it will function similarly to 'Estonia 2007', 'Stuxnet', or 'cyber Pearl Harbor' in reporting.

Hypothetically, we could imagine a future article in a paper like *The Guardian* on cyber conflict that would include a touchpoint along the lines of 'the Russia-Ukraine War revealed the limited role of cyber conflict in modern warfare'. However, as the analysis of the Estonia case study above suggested, the meanings encoded in such touchpoints are not fixed and can change over time or be actively reinterpreted.

As indicated by the role of *The New York Times'* reporting on Stuxnet in the shaping of wider coverage, it is likely that some sources will come to play an outsize role in the framing of the cyber aspects of the Russia-Ukraine War. Microsoft's public reports on the role of Russian cyber operations in the conflict are credible candidates for playing such a role ('Defending Ukraine: Early Lessons from the Cyber War' 2022; 'The Hybrid War in Ukraine' 2022). The second of the two reports combined both cyber operations and disinformation under the term 'hybrid war'. It is too early to say whether the prominence of that report will lead to journalistic coverage of the cyber aspects of the Russia-Ukraine War adopting a similar framing. Equally, it is entirely possible that those reports will drop out of future media coverage entirely.

Future work

Further work could expand the range of news organisations covered in our analysis. We observed anecdotally that tabloid coverage of cyber conflict differs from the broadsheet coverage. More broadly, our focus was on the text of the articles we examined; further work could examine the visual presentation of reporting.

A quantitative content analysis of the material in our sample could trace how often different individuals and companies are cited as experts, enabling further analysis of how the changing mixture of experts cited in reporting shapes the way these events are covered. Equally,

qualitative research based on engagement with, or observation of, the people producing this coverage would complement our analysis of the textual outputs.

Further work could explore the reasons why certain framings become more widely adopted than others. This could also explore whether the intangible nature of cyber conflict (Stevens 2020, 136) makes it a subject where journalists are especially dependent on framing devices. Moreover, this could extend to explore other, similar analogous framings that did not achieve widespread usage. For instance, we found a series of articles referencing 'space Pearl Harbor' (see amongst others Tisdall 2001; Norton-Taylor 2001; Wilsdon 2004), an analogy designed to evoke similar fears, emanating from similar policymakers. Additional research could further explore the use of the 'Pearl Harbor' suffix.

Conclusion

In this article we have used framing theory to analyse how historical events and analogy are used to interpret incidents of cyber conflict. Journalists are often not subject matter experts and for mainstream publications they are not writing for an expert audience. Novel or hard to understand events – such as cyber conflict – are presented in news reporting through framing them in the context of more familiar events. Over time, some of those events in turn become touchpoints that are used to frame new developments.

We also briefly examined how this framing involves a social process of translation derived from interactions between often competing interpreters and interpretations among academics, practitioners, and journalists. Through observing interactions between these actors, we attempt to recognise the patterns and implications of relations in networks of knowledge formation. Such instances should not be seen in isolation, but as part of a broader network of interactions which over time come to form knowledge about cyber conflict.

Journalism is one part of wider socio-political processes of knowledge production and accordingly there will be overlaps between the processes whose outputs we have examined in this paper and other forms of knowledge production. One of the key differences between journalism and other forms of knowledge production is that meanings may be 'stickier' due to the limited wordcount available and the consequent reliance on 'touchpoint'-type descriptions of events. This means that events come to have simplified meanings in media reporting. At the

same time, these meanings may shift as new developments lead journalists to reframe these touchpoints.

For observers without access to primary sources on cyber operations, news media reporting will remain an important source. That academics sometimes bemoan the quality of mainstream news media reporting on cyber conflict may itself be a sign of how often we return to these sources in our work. Understanding how the dynamics of this form of knowledge production shape these outputs is therefore important for critical reflection on our own understanding of cyber conflict.

[5,937 words]

Bibliography

Altheide, David L. 1997. 'The News Media, the Problem Frame, and the Production of Fear'. *The Sociological Quarterly* 38 (4): 647–68.

Ars Staff. 2018. 'Bloomberg: Super Micro Motherboards Used by Apple, Amazon Contained Chinese Spy Chips'. Ars Technica. 4 October 2018. https://arstechnica.com/gadgets/2018/10/bloomberg-super-micro-motherboards-used-by-apple-amazon-contained-chinese-spy-chips/.

Belfer Center, dir. 2014. *America's Cyber Pearl Harbor: Edward Snowden*. https://www.youtube.com/watch?v=XRqSSyCyEz4.

Bendrath, Ralf, Johan Eriksson, and Giampiero Giacomello. 2007. 'From 'Cyberterrorism'to "Cyberwar", Back and Forth: How the United States Securitized Cyberspace'. In *International Relations and Security in the Digital Age*, 77–102. Routledge.

Bennett, W. Lance, and Regina G. Lawrence. 1995. 'News Icons and the Mainstreaming of Social Change'. *Journal of Communication* 45 (3): 20–39. https://doi.org/10.1111/j.1460-2466.1995.tb00742.x.

Broad, William J., John Markoff, and David E. Sanger. 2011. 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay'. *The New York Times*, 15 January 2011, sec. World. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Cavelty, Myriam Dunn. 2008. 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate'. *Journal of Information Technology & Politics* 4 (1): 19–36. https://doi.org/10.1300/J516v04n01_03.

'Defending Ukraine: Early Lessons from the Cyber War'. 2022. Microsoft On the Issues. 22 June 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Farivar, Cyrus. 2009. 'A Brief Examination of Media Coverage of Cyberattacks (2007–Present)'. In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 182–88. IOS Press.

Farrell. 2013. 'Cyber-Pearl Harbor Is a Myth'. *Washington Post*, 11 November 2013. https://www.washingtonpost.com/news/monkey-cage/wp/2013/11/11/cyber-pearl-harbor-is-a-myth/.

Franceschi-Bicchierai, Lorenzo. 2022. 'Inside Ukraine's Decentralized Cyber Army'. 19 July 2022. https://www.vice.com/en/article/y3pvmm/inside-ukraines-decentralized-cyber-army?utm_source=substack&utm_medium=email.

Gamson, William A., and Andre Modigliani. 1989. 'Media Discourse and Public Opinion on Nuclear Power: A Constructionist Approach'. *American Journal of Sociology* 95 (1): 1–37. https://doi.org/10.1086/229213.

Gartzke, Erik. 2013. 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth'. *International Security* 38 (2): 41–73. https://doi.org/10.1162/ISEC_a_00136.

Goffman, Erving. 1974. *Frame Analysis: An Essay on the Organization of Experience.* Harvard University Press.

Goldman, Emily O, and John Arquilla. 2014. 'Cyber Analogies'. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Horkos 🌻 [@WylieNewmark]. 2020. '@KimZetter @RidT Strong Agree with @RidT. It's a Little Embarrassing to See so Many People Disagreeing, Apparently Laying Bare That They Likely Don't Understand the Differences between CNE and CNA as Technical and Operational Concepts.' Tweet. *Twitter*. https://twitter.com/WylieNewmark/status/1338583285815865344.

Jarvis, L, S Macdonald, and A Whiting. 2016. 'Analogy and Authority in Cyberterrorism Discourse: An Analysis of Global News Media Coverage'. *Global Society* 30 (4): p605-623.

Johnson, William R. 2009. *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer*. Georgetown University Press.
Kim Zetter [@KimZetter]. 2020. 'Do You Agree with @Ridt That Exfiltrating Data from a Regular Foreign Intel Target — However Stealthy, Targeted, or Labor-Intensive — Should Not Be Called an "Attack" and That an Intrusion Only Becomes an Attack When Adversaries Modify, Delete, or Leak Files?' Tweet. *Twitter*. https://twitter.com/KimZetter/status/1338558312279724032.
Kitzinger, Jenny. 2000. 'Media Templates: Patterns of Association and the (Re)Construction of Meaning over Time'. *Media, Culture & Society* 22 (1): 61–84. https://doi.org/10.1177/016344300022001004.
———. 2007. 'Framing and Frame Analysis'. *Media Studies: Key Issues and Debates. London, UK: Sage*, 134–61.
Koenig, Thomas. n.d. 'Frame Analysis: A Primer (Thomas Koenig)'. Accessed 16 August 2022. https://www.restore.ac.uk/lboro/resources/links/frames_primer.php.
Lawson, Sean, and Michael K. Middleton. 2019. 'Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016'. *First Monday*, March. https://doi.org/10.5210/fm.v24i3.9623.
Manjoo, Farhad. 2022. 'Opinion | The Ukrainian Cyberwar That Wasn't'. *The New York Times*, 11 March 2022, sec. Opinion. https://www.nytimes.com/2022/03/11/opinion/russia-ukraine-cyberattacks.html.
Martin, Ciaran. 2022. 'Cyber Realism in a Time of War'. Lawfare. 2 March 2022. https://www.lawfareblog.com/cyber-realism-time-war.
Nicole Perlr🌻th [@nicoleperlroth]. 2020. '@KimZetter I've Never Agreed with Rid on His Specific Terminology for Attack, "Cyberwar" Etc. I Also Think It Downplays What We Are Currently Witnessing.' Tweet. *Twitter*. https://twitter.com/nicoleperlroth/status/1338557856765734912.
Pan, Zhongdang, and Gerald M. Kosicki. 1993. 'Framing Analysis: An Approach to News Discourse'. *Political Communication* 10 (1): 55–75. https://doi.org/10.1080/10584609.1993.9962963.
Pieri, Elisa. 2019. 'Media Framing and the Threat of Global Pandemics: The Ebola Crisis in UK Media and Policy Response'. *Sociological Research Online* 24 (1): 73–92. https://doi.org/10.1177/1360780418811966.
Rid, Thomas. 2022. 'Opinion | Why You Haven't Heard About the Secret Cyberwar in Ukraine'. *The New York Times*, 18 March 2022, sec. Opinion. https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html.
Stevens, Clare. 2020. 'Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet'. *Contemporary Security Policy* 41 (1): 129–52. https://doi.org/10.1080/13523260.2019.1675258.
'The Hybrid War in Ukraine'. 2022. Microsoft On the Issues. 27 April 2022. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/.
Thomas Rid [@RidT]. 2020. 'Also, a Subtle Point on Terminology: Exfiltrating Data from Regular Foreign Intelligence Targets — However Stealthy, Targeted, or Labor-Intensive — Should Not Be Called an "Attack." An Intrusion Becomes an Attack When Adversaries Modify, Delete, or Leak Targeted Files.' Tweet. *Twitter*. https://twitter.com/RidT/status/1338537697560965120.
Vliegenthart, Rens, and Liesbet van Zoonen. 2011. 'Power to the Frame: Bringing Sociology Back to Frame Analysis'. *European Journal of Communication* 26 (2): 101–15. https://doi.org/10.1177/0267323111404838.
Wirtz, James J. 2017. 'The Cyber Pearl Harbor'. *Intelligence and National Security* 32 (6): 758–67. https://doi.org/10.1080/02684527.2017.1294379.

Articles from *The Guardian*

Arthur, Charles. 2008. ‘That Cyberwarfare by Russia on Estonia? It Was One Kid.. in Estonia’. *The Guardian*, 25 January 2008, sec. Technology. https://www.theguardian.com/technology/blog/2008/jan/25/thatcyberwarfarebyrussiaon.

———. 2011. ‘Iran Should Investigate Stuxnet Virus, Says Atomic Chief’. *The Guardian*, 4 February 2011, sec. World news. https://www.theguardian.com/world/2011/feb/04/iran-stuxnet-virus.

Beaumont, Peter. 2010a. ‘Iran Nuclear Experts Race to Stop Spread of Stuxnet Computer Worm’. *The Guardian*, 25 September 2010, sec. World news. https://www.theguardian.com/world/2010/sep/26/iran-stuxnet-worm-nuclear.

———. 2010b. ‘Stuxnet Worm Heralds New Era of Global Cyberwar’. *The Guardian*, 30 September 2010, sec. Technology. https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar.

———. 2010c. ‘Iran “detains Western Spies” after Cyber Attack on Nuclear Plant’. *The Guardian*, 2 October 2010, sec. World news. https://www.theguardian.com/world/2010/oct/02/iran-western-spies-cyber-attack.

Bentley, Alan. 2013. ‘Is Armageddon on the Cyber Horizon?’ *The Guardian*, 17 April 2013, sec. Media Network. https://www.theguardian.com/media-network/media-network-blog/2013/apr/17/cyber-attack-armageddon-protection.

Borger, Julian. 2000. ‘US Mounts $2bn Offensive against Cyber-Terrorists’. *The Guardian*, 8 January 2000, sec. World news. https://www.theguardian.com/world/2000/jan/08/terrorism.

———. 2010. ‘Iran Halted Its “top Priority” Uranium Enrichment Due to Technical Problems’. *The Guardian*, 23 November 2010, sec. World news. https://www.theguardian.com/world/2010/nov/23/iran-uranium-halt-iaea-enrichment.

———. 2011. ‘Iran’s Nuclear Activity under Scrutiny as Evidence of Weapons Threat Emerges’. *The Guardian*, 2 November 2011, sec. World news. https://www.theguardian.com/world/2011/nov/02/iran-nuclear-weapons-programme.

———. 2016. ‘“Trident Is Old Technology”: The Brave New World of Cyber Warfare’. *The Guardian*, 16 January 2016, sec. Technology. https://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare.

Borger, Julian, and Saeed Kamali Dehghan. 2010a. ‘Attack on Iranian Nuclear Scientists Prompts Hit Squad Claims’. *The Guardian*, 29 November 2010, sec. World news. https://www.theguardian.com/world/2010/nov/29/iranian-nuclear-scientists-attack-claims.

———. 2010b. ‘Covert War against Iran’s Nuclear Aims Takes Chilling Turn’. *The Observer*, 5 December 2010, sec. World news. https://www.theguardian.com/world/2010/dec/05/iran-nuclear-experts-killings.

———. 2011. ‘Iranian Nuclear Scientist “Tortured on Suspicion of Revealing State Secrets”’. *The Guardian*, 4 January 2011, sec. World news. https://www.theguardian.com/world/2011/jan/04/iranian-nuclear-scientist-tortured-claim.

Borger, Julian, and diplomatic editor. 2014. ‘Russians Open New Front after Estonian Official Is Captured in “Cross-Border Raid”’. *The Guardian*, 7 September 2014, sec. World news. https://www.theguardian.com/world/2014/sep/07/russia-parades-detained-estonian-police-officer.

Bradbury, Danny. 2009. ‘The Fog of Cyberwar’. *The Guardian*, 5 February 2009, sec. Technology. https://www.theguardian.com/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access.
Burke, Jason. 2007. ‘Europe Shivering in the New Cold War’. *The Observer*, 2 June 2007, sec. World news. https://www.theguardian.com/world/2007/jun/03/eu.russia.
Butcher, Mike. 2002. ‘Cyber Hype’. *The Guardian*, 5 December 2002, sec. Technology. https://www.theguardian.com/technology/2002/dec/05/onlinesupplement.
Campbell, Duncan. 1999. ‘Cyber Sillies’. *The Guardian*, 20 May 1999, sec. UK news. https://www.theguardian.com/uk/1999/may/20/military.defence.
Carroll, Rory. 2012. ‘US Urged to Recruit Master Hackers to Wage Cyber War on America’s Foes’. *The Guardian*, 10 July 2012, sec. Technology. https://www.theguardian.com/technology/2012/jul/10/us-master-hackers-al-qaida.
Coulter, Michael. 2021. ‘“Accident” at Iran’s Natanz Nuclear Plant as New Uranium Enrichment Starts’. *The Guardian*, 11 April 2021, sec. World news. https://www.theguardian.com/world/2021/apr/11/accident-at-irans-natanz-nuclear-plant-as-new-uranium-enrichment-starts.
Coviello, Art. 2013. ‘How Technology Is Changing the Way We Think about Security’. *The Guardian*, 23 April 2013, sec. Media Network. https://www.theguardian.com/media-network/media-network-blog/2013/apr/23/technology-big-data-information-security.
Glenny, Misha. 2009. ‘Cyber Armies Are Gearing up in the Cold War of the Web’. *The Guardian*, 25 June 2009, sec. Opinion. https://www.theguardian.com/commentisfree/2009/jun/25/cybercrime-nato-cold-war.
Grassegger, Hannes, and Mikael Krogerus. 2017. ‘Fake News and Botnets: How Russia Weaponised the Web’. *The Observer*, 2 December 2017, sec. Technology. https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia.
Greenwald, Glenn. 2013. ‘Pentagon’s New Massive Expansion of “cyber-Security” Unit Is about Everything except Defense’. *The Guardian*, 28 January 2013, sec. Opinion. https://www.theguardian.com/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet.
Halliday, Josh. 2010a. ‘Stuxnet Worm Is the “Work of a National Government Agency”’. *The Guardian*, 24 September 2010, sec. Technology. https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency.
———. 2010b. ‘Stuxnet Worm Is Aimed to Sabotage Iran’s Nuclear Ambition, New Research Shows’. *The Guardian*, 16 November 2010, sec. Technology. https://www.theguardian.com/technology/2010/nov/16/stuxnet-worm-iran-nuclear.
———. 2011. ‘WikiLeaks: US Advised to Sabotage Iran Nuclear Sites by German Thinktank’. *The Guardian*, 18 January 2011, sec. US news. https://www.theguardian.com/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear.
Halliday, Josh, and Julian Borger. 2010. ‘Iranian Nuclear Plants Likely Target of Foiled Cyber Sabotage’. *The Guardian*, 25 September 2010, sec. World news. https://www.theguardian.com/world/2010/sep/25/iran-cyber-hacking-nuclear-plants.
Harding, Luke. 2007. ‘Protest by Kremlin as Police Quell Riots in Estonia’. *The Observer*, 29 April 2007, sec. World news. https://www.theguardian.com/world/2007/apr/29/russia.lukeharding.
Hencke, David. 2009. ‘Whitehall Plans New Cyber Security Centre to Deter Foreign Hackers’. *The Guardian*, 14 June 2009, sec. Technology. https://www.theguardian.com/technology/2009/jun/14/government-security-cyber-crime-hacking.
Hinsliff, Gaby. 2008. ‘MI5 Seeks Powers to Trawl Records in New Terror Hunt’. *The Observer*,

16 March 2008, sec. UK news. https://www.theguardian.com/uk/2008/mar/16/uksecurity.terrorism.
Hopkins, Nick. 2011a. 'Stuxnet Attack Forced Britain to Rethink the Cyber War'. *The Guardian*, 30 May 2011, sec. Politics. https://www.theguardian.com/politics/2011/may/30/stuxnet-attack-cyber-war-iran.
———. 2011b. '"New Stuxnet" Worm Targets Companies in Europe'. *The Guardian*, 19 October 2011, sec. Technology. https://www.theguardian.com/technology/2011/oct/19/stuxnet-worm-europe-duqu.
Hunker, Jeffrey. 2011. 'Deterrence Won't Stop Cyber-Attacks'. *The Guardian*, 7 June 2011, sec. Opinion. https://www.theguardian.com/commentisfree/cifamerica/2011/jun/07/pentagon-cyber-attack-war.
Javedanfar, Meir. 2011. 'Iran Will Stay Tough on Nuclear'. *The Guardian*, 18 January 2011, sec. Opinion. https://www.theguardian.com/commentisfree/2011/jan/18/iran-nuclear-talks-regime.
Johnson, Bobbie. 2008. 'Nato Says Cyber Warfare Poses as Great a Threat as a Missile Attack'. *The Guardian*, 6 March 2008, sec. Technology. https://www.theguardian.com/technology/2008/mar/06/hitechcrime.uksecurity.
———. 2009. 'Is China Stepping towards Cyberwar?' *The Guardian*, 30 March 2009, sec. Technology. https://www.theguardian.com/technology/blog/2009/mar/30/internet-computing.
Kingsley, Patrick. 2012. 'How Tiny Estonia Stepped out of USSR's Shadow to Become an Internet Titan'. *The Guardian*, 15 April 2012, sec. Technology. https://www.theguardian.com/technology/2012/apr/15/estonia-ussr-shadow-internet-titan.
Kiss, Jemima. 2012. 'Who Controls the Internet?' *The Guardian*, 17 October 2012, sec. Technology. https://www.theguardian.com/technology/2012/oct/17/who-rules-internet.
MacAskill, Ewen. 2011a. 'Stuxnet Cyberworm Heads off US Strike on Iran'. *The Guardian*, 16 January 2011, sec. Technology. https://www.theguardian.com/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran.
———. 2011b. 'US Calls on Its Nato Partners to Help Resist Cyber-Attacks'. *The Guardian*, 16 May 2011, sec. Technology. https://www.theguardian.com/technology/2011/may/17/us-nato-cyber-attacks-report.
Macqueen, Angus. 2008. 'The Russians Are Back'. *The Guardian*, 23 February 2008, sec. Books. https://www.theguardian.com/books/2008/feb/23/politics1.
Meghani, Sagar, Nasser Karimi, and Associated Press. 2010. 'Anti-Iran Computer Bug Had Powerful Backers'. *The Guardian*, 26 September 2010, sec. World news. https://www.theguardian.com/education/2010/sep/26/iran-computer-bug-attcks-nuclear-plants.
Naughton, John. 2010a. 'Meet the Stuxnet, so Much Subtler than a Tactical Nuclear Device'. *The Guardian*, 16 October 2010, sec. Technology. https://www.theguardian.com/technology/2010/oct/17/stuxnet-worm-john-naughton.
———. 2010b. 'How Do We Counter Cyber Attack? That's the £500m Question'. *The Guardian*, 30 October 2010, sec. Technology. https://www.theguardian.com/technology/2010/oct/31/cyber-attack-networker-military.
Norton-Taylor, Richard. 2001. 'Bush Plans to Test Space-Based Laser Weapons'. *The Guardian*, 19 July 2001, sec. World news. https://www.theguardian.com/world/2001/jul/19/usa.richardnortontaylor.
———. 2010. 'Top-Tier Threats to Britain's Security'. *The Guardian*, 18 October 2010, sec. Politics. https://www.theguardian.com/politics/2010/oct/18/top-tier-threats-to-britain.
Paul, Kari. 2022a. '"Catastrophic" Cyberwar between Ukraine and Russia Hasn't Happened (yet), Experts Say'. *The Guardian*, 9 March 2022, sec. Technology.

https://www.theguardian.com/technology/2022/mar/09/catastrophic-cyber-war-ukraine-russia-hasnt-happened-yet-experts-say.
———. 2022b. ‘Russia’s Slow Cyberwar in Ukraine Begins to Escalate, Experts Say’. *The Guardian*, 2 April 2022, sec. World news. https://www.theguardian.com/world/2022/apr/01/russia-ukraine-cyberwar.
Rojas, Peter. 2003. ‘The Paranoia That Paid Off’. *The Guardian*, 24 April 2003, sec. Technology. https://www.theguardian.com/technology/2003/apr/24/security.newmedia.
Ross, Dickon. 2003. ‘Electronic Pearl Harbor’. *The Guardian*, 20 February 2003, sec. Technology. https://www.theguardian.com/technology/2003/feb/20/security.onlinesupplement.
Rushe, Dominic, and Spencer Ackerman. 2015. ‘Obama Plans for Cybersecurity Aim “to Make Internet Safer Place”’. *The Guardian*, 21 January 2015, sec. US news. https://www.theguardian.com/us-news/2015/jan/20/obama-cybersecurity-state-of-the-union-address-speech.
Safi, Michael, and Rosie Scammell. 2020. ‘Iran Admits Incident at Natanz Nuclear Site Caused Major Damage’. *The Guardian*, 5 July 2020, sec. World news. https://www.theguardian.com/world/2020/jul/05/satellite-image-raises-suspicions-of-attack-at-iran-nuclear-site.
Somaiya, Ravi. 2008. ‘Defenders of Cyberspace’. *The Guardian*, 1 October 2008, sec. Technology. https://www.theguardian.com/technology/2008/oct/02/4.
Sparrow, Andrew. 2010. ‘David Cameron Plans New Centre to Fight Cyber Attacks’. *The Guardian*, 15 January 2010, sec. Politics. https://www.theguardian.com/politics/2010/jan/15/cameron-cyber-attacks-centre.
Sweney, Mark. 2007. ‘Is Eastern Europe’s Cyberwar the Shape of Things to Come?’ *The Guardian*, 17 May 2007, sec. News. https://www.theguardian.com/news/blog/2007/may/17/easterneuropes.
The Guardian. 1999. ‘Hacker in Shackles’. *The Guardian*, 10 August 1999, sec. US news. https://www.theguardian.com/theguardian/1999/aug/10/features11.g22.
Timm, Trevor. 2014. ‘The Senate Is Giving More Power to the NSA, in Secret. Everyone Should Fight It’. *The Guardian*, 12 July 2014, sec. Opinion. https://www.theguardian.com/commentisfree/2014/jul/12/senate-nsa-secret-cybersecurity-information-sharing-act.
Tisdall, Simon. 2001. ‘Fear of Attack Triggers Arms Build-Up’. *The Guardian*, 13 January 2001, sec. World news. https://www.theguardian.com/world/2001/jan/13/usa.simontisdall.
Tran, Mark. 2007. ‘China Denies Hacking the Pentagon’. *The Guardian*, 4 September 2007, sec. World news. https://www.theguardian.com/world/2007/sep/04/china.usa.
Traynor, Ian. 2007. ‘Russia Accused of Unleashing Cyberwar to Disable Estonia’. *The Guardian*, 17 May 2007, sec. World news. https://www.theguardian.com/world/2007/may/17/topstories3.russia.
Wilsdon, James. 2004. ‘Mission to Planet Rumsfeld’. *The Guardian*, 1 March 2004, sec. Science. https://www.theguardian.com/science/2004/mar/01/spaceexploration.usnews.