The technopolitics of cybersecurity

Sociotechnical configurations, epistemic devices, and the production of knowledge

Aanonsen, C.E.

Publication date
2025

6

Chapter six: Stuxnet and the discursive production of cybersecurity[26]

Box 6.1 The role of discourse in sociotechnical configurations

Stuxnet – the infamous malware described in the introduction of this thesis – is still discussed as one of the most destructive cyberattacks to date. This empirical analysis differs from the previous Chapters 3, 4, and 5 since it does not explicitly explore a particular sociotechnical configuration. However, it shows the role of discourse in the propagation of cybersecurity as it has emerged as a pivotal notion in the lexicon of orthodox International Relations (IR), hereunder Strategic Studies. The chapter outlines academic, media, and political attention to scenarios of 'cyber war' after the discovery of Stuxnet, and how this has shaped contemporary understandings of what cybersecurity is, and does, as a so-called deterrent or strategic tool for states. The imaginaries that commenced in the wake of Stuxnet cannot be seen as isolated or collective ideas, but as historically and politically situated. Hence, this chapter analyses the importance of discourse and how dominant perspectives devised in academia continue to inform the commercial design, maintenance, and development of technical systems and capabilities to 'achieve' cybersecurity for states. On the one hand, the chapter emphasises the role of discourse and how it can be activated within a particular sociotechnical configuration. On the other hand, in its independent contribution as it is also intended, I encourage scholars of security to critically challenge the promises of 'new' technologies (such as the thrills and terrors of artificial intelligence) and how they emerge as potential threats and/or 'strategic' capabilities.

[26] With some minor formatting (e.g., editing section titles) and grammatical edits (e.g., 'article' has been replaced by 'chapter'), this chapter was previously published as: Aanonsen, C. E. (2025) 'Stuxnet, revisited (again): producing the strategic relevance of cyber operations', *Journal of Cyber Policy*, pp. 1–17. Available at: https://doi.org/10.1080/23738871.2025.2492570.

6.1 Introduction

The Stuxnet malware that hit Iran in the late 2000s was unlike anything the world had ever seen before. When it became publicly known in 2010, the major damage to the centrifuges at the Natanz uranium enrichment facility was astonishing for many, especially considering the complexity of the state-sponsored cyber operation.[27] Since then, it has undoubtedly affected the understanding of cyber capabilities and of cyber operations as a tool for achieving strategic objectives. This is largely due to how Stuxnet catalysed the trajectory of academic debates on how to study the phenomenon of 'cyber' as a multifaceted component of international relations and security. Particularly embraced by orthodox security studies, these perspectives continue to influence American and Western policy objectives based on the imagined utility of cyber operations as an instrument of power.

This chapter argues that Stuxnet and its aftermath can be perceived as having spurred a discursive paradigm shift for imaginaries of the strategic 'utility' of cyber capabilities and operations. In arguing that Stuxnet is due a revisit, the novelty of this contribution is that it reflects upon the epistemic interplay of knowledge and materiality as conditions for political action. Critical perspectives pay attention to the underpinning of knowledge and expertise that produces notions of 'strategic relevance' in the first place. This calls for a critical review of the production of the 'strategic relevance' of cyber operations that has largely been driven by the academic discourse in orthodox perspectives on strategic security and its impact on international politics.

Although Stuxnet has time and again been a focal point in research on offensive cyber operations in International Relations (IR) and the field of Strategic Studies, it is due time that Stuxnet is revisited (again). Owing to continuous claims that suggest that the role and utility of cyber operations in international conflict has been solved, I foreground these perspectives as manufacturing discourse that in turn produces political possibilities and thus 'strategic relevance'. By zooming into the vast literature that has grown over the past decade, I shed light on contributions that view cyber operations such as Stuxnet as a less escalatory option than conventional military force yet sufficiently 'potent' as an alternative

[27] The research article upon which this Chapter is based on was published before Israeli and the U.S. attacks on Iran (including the Natanz nuclear facility), which are still ongoing at of the time of writing (June 2025). These attacks are not referenced in this Chapter.

to diplomatic means. For example, in the context of the longstanding conflict between the US/Israel and Iran, cyber operations have been regarded as functioning as 'substitutions' for conventional military force. These perspectives stress a belief that to avoid conflict escalation, operations such as Stuxnet are a viable option somewhere between diplomacy and military action (Borghard and Lonergan, 2019; Healey and Singh, 2022; Valeriano and Maness, 2018), e.g., as a mechanism of 'pressure-release' (Healey and Jervis, 2020).

Taking these perspectives into consideration, I do not aim to debate the strategic utility of Stuxnet or cyber operations and capabilities in general. Rather, I show another side of the coin, arguing that strategic relevance does not exist of its own accord. It is produced from assumptions about utility based on previous experiences, discursive interactions, technical capabilities, and political will. In other words, the strategic relevance of cyber operations and capabilities are historically and politically produced, situated in sociotechnical configurations. As such, Stuxnet represents a paradigm shift with respect to how its discovery led to the development of a subfield of academic research that continues to discursively produce imaginaries of strategic utility of cyber capabilities, subsequently translating into policy and strategic thinking.

The chapter proceeds by highlighting influential academic contributions on the strategic relevance of cyber operations in Section 6.2. I emphasise the significance of Stuxnet as paramount to the trajectory of these debates and the conviction of danger associated with cyber capabilities that are also, at the same time, understood as useful strategic tools. The chapter continues in Section 6.3 with a breakdown of Stuxnet and its aftermath to refresh the memory of a fragmented story about what is still referred to as 'the World's First Digital Weapon' (Zetter, 2014; Sanger, 2018). With this in mind, I proceed to a twofold analysis. First, in Section 6.4, I explore how Stuxnet has produced imaginaries of cyber operations as a substitute for conventional military force and the conditions conducive to this. Second, in Section 6.5, I reflect upon the epistemic interplay of discourses, knowledge and technical capabilities as conditioning political action following Stuxnet. I then arrive at a point that addresses how Stuxnet represents a paradigmatic shift in imaginaries that continuously (re)produce the 'strategic relevance' of cyber operations. The aim is to better equip scholars with tools to grapple with the historical and social production of 'new' strategic capabilities that continue to shape academic scholarship and, concurrently, international politics.

6.2 The strategic relevance of cyber operations

Today, most states have to some capacity developed defensive capabilities to protect digital critical infrastructure. Numerous states have also invested in offensive cyber capabilities as part of deterrence strategies or as weapons to achieve intelligence, security or war objectives (Fanelli, 2016). At the 2016 NATO summit in Warsaw, the cyber domain was declared a fifth domain of operations on a par with land, sea, air and space. The rearmament of cyber capabilities can be understood as vital for how policy strategists understand conflict and so-called escalation dynamics today (Libicki and Tkacheva, 2020). There is also a common agreement in traditional security perspectives that cyber operations carried out by states usually take place as larger cross-domain operations aimed at espionage or to conduct sabotage (Schulze et al., 2020). I foreground the discovery of Operation Olympic Games as the starting point for these measures.[28] Diving into the trajectory of the academic debate tells a story about how imaginaries of cyber capabilities have been stabilised over time and made possible the acceptance of the cyber domain as a domain of warfare.

The Stuxnet malware was mainly developed by the U.S. and Israel with the goal of weakening Iran’s nuclear programme through perpetual sabotage (Sanger, 2012; Zetter, 2014). Stuxnet caught global attention as it was depicted as digital malware that could not only sabotage the functionality of infrastructure but also cause severe destruction. Thus, when Operation Olympic Games became widely known in 2010, it represented a seemingly unique phenomenon that caused public uproar. Many feared that ‘cyber Pearl Harbour’ would occur, and that the world was on the brink of cyberwar (Sanger, 2018; Lindsay, 2013, 373). Although it has since been agreed in Strategic Studies that this scenario was far less realistic than initially feared (see Rid, 2012, 2013; Smeets and Soesanto, 2020; Maschmeyer, 2021), many still consider the potential for damage caused by cyberattacks to be much more significant than before 2010.

The ongoing academic debate in Strategic Studies and orthodox security studies on the strategic utility of cyber operations is in part oriented towards questioning to what extent cyber operations are a significant factor in international relations or remain a

[28] Operation Olympic Games was the US-led coalition operation that deployed Stuxnet, the malware that corrupted control systems at Natanz.

peripheral issue. Lennart Maschmeyer argues in favour of the latter, namely that the strategic utility of cyber 'weapons' is limited due to the inherent constraints of a 'subversive trilemma' – trade-offs between speed, intensity and control (Maschmeyer, 2021, 2022).[29] He argues that enhancing one of these options is likely to reduce the effectiveness of the other two. Maschmeyer claims that cyber operations 'will tend to be too slow, too low in intensity, or too unreliable to provide significant utility' (Maschmeyer, 2021, p. 66). Furthermore, he anticipates that states primarily utilise cyber operations independently rather than in conjunction with diplomacy or conventional warfare, first and foremost as part of covert campaigns targeting non-military entities (Maschmeyer, 2021). In contrast, Jason Healey argues that while the trilemma accurately depicts challenges related to cyber operations, this view does not capture their broader strategic potential (Healey, 2022). Healey highlights that cyber operations can target multiple systems at once and that they can have a widespread significant impact. He also notes that the cumulative impact of repeated cyber operations, along with technological advancement and geopolitical shifts, need to be considered when assessing utility and strategic relevance. This might enhance the effectiveness of cyber operations more than the trilemma/quadrilemma model suggests:

> Cyber operations seem to be largely subversion […] only because states haven't been willing to play for higher stakes. Now that Russia has again invaded Ukraine – and is worried about regime failure and making nuclear threats – it and other states may decide to undertake riskier operations, to strive for worse effects than those analysed by Maschmeyer and other researchers. (Healey, 2022)

When considered as an operational theatre, we are often told that the cyber domain is fundamentally different from the conventional domains of sea, land, air and space. In comparison to an airstrike, for example, the intention behind cyberattacks is said to appear far less unequivocal to a victim for several reasons. Confusion and potential misinterpretations about the objective and purpose of an attack can occur in the affected party due to the possibly concealed traces and origin of malware. The intention of the attacker, whether a state or non-state actor, does not always harmonise with the opinion of the victim (Libicki and Tkacheva, 2021; Schulze et al., 2020). Consequently, how cyber capabilities affect conflict levels and escalation is not always analysed in isolation from conventional warfare nor from general interstate dynamics. Jason Healey and Robert Jervis'

---

[29] In his article in *Lawfare* (2022), Maschmeyer expands the trilemma to a quadrilemma by adding secrecy as a fourth factor at odds with demands of speed, intensity and control.

(2020) notion of 'pressure-release' builds on their observation that cyber operations can in some circumstances act as a form of relief from escalatory dynamics. This can, they argue, occur when cyber operations are utilised *instead* of resorting to conventional military force and fulfilling expectations of state action (Healey and Jervis, 2020).

'Escalation' has traditionally been understood as actions or threats that contribute to increasing the intensity of conflict between parties (Schulze et al. , 020). Herman Kahn's (1965) concept of the escalation ladder is illustrative of this understanding within traditional security studies based on a rational actor model. The escalation ladder is explained as a hierarchy of conflict levels, where states can climb both up and down the 'ladder' (Kahn, 1965). In this view, states can also stay at a mutually proportional level, which has become known as 'tit-for-tat' (Schulze et al., 2020). Stuxnet, interpreted through the lens of these dominant theoretical frameworks, has to a large extent been viewed as the origin of cyber-related security dilemmas and subsequent rearmament carrying potential for escalation (Segal, 2016; Healey and Singh, 2022). Within strategic studies literature, these scholars are considered to have brought important contributions to the table with regard to the role of cyber operations. What can in turn be gathered from these perspectives, however, is the imaginaries of the utility of such operations. In other words, these theoretical perspectives represent particular ways of analysing the world that constrain what conditions are considered conductive to cyber operations by characterising them as strategically relevant in their own right.

There are, indeed, conspicuous problems that surface when trying to fit cyber operations into established frameworks for the strategic analysis of conflict escalation. As pointed out by critical scholarship on security, these problems are in part due to the ambiguous understandings of cyber operations concerning precisely what threatens, against whom and what effects it can have (Dunn Cavelty, 2013, 2018) – also, perhaps more importantly, how threat knowledge is drawn from discourses that contribute to inflation in both public and private military investments and expenditures, as well as technological innovation and particular methods, mechanisms and policies for handling threat. In this view, material characteristics become visible, as well as how they co-produce knowledge and political action (Balzacq and Dunn Cavelty, 2016; Stevens, 2020). As the next sections show, Stuxnet played an imperative role in producing the foundational knowledge that scholars and practitioners obtain, produce and disseminate about offensive and defensive cyber capabilities. The following Section 6.3 provides an account of known occurrences that have thus far constituted the grand narrative of Stuxnet. Taking into consideration the highly sensitive and classified nature of Operation Olympic Games, the record of it suffers from opaque and selectively available sources. Nevertheless, owing to unremitting investigative journalism and eventually declassified documents, new sources continually materialise. To fill gaps in the story of Stuxnet, it is useful to provide the following brief recital of the known events as historical context for the analysis.

6.3 Stuxnet and the paradigm shift

Cyber operations conducted by states were not considered a new phenomenon when Stuxnet was discovered in 2010. Many have agreed that Moonlight Maze was the first state-sponsored cyber operation. From 1996 to 1998, hackers stole thousands of sensitive documents from the American government and military institutions. The operation was attributed to Russia (Buchanan, 2020). Another known instance occurred when the American weapons industry and other public institutions were hit by a series of data breaches between 2003 and 2006. The attacks were nicknamed Titan Rain and attributed to China (Council on Foreign Relations, n.d., a; Buchanan, 2017). Similarly, Estonian organizations and government agencies were in 2017 subject to distributed denial-of-service (DDoS) attacks with a probable origin from Russian security authorities. The attacks were limited to leaks of classified information and the reduced functionality of public IT systems. Traditional malware such as DDoS attacks, trojan horses, keyloggers and spyware do not effectively cause kinetic damage. Stuxnet differed significantly from these attacks as it was a highly specialised coalition operation that was said, as mentioned, to have been deployed as an alternative to other means in a politically tense situation between states (Sanger, 2018). This substantiated the conceptualisation of Stuxnet as 'weaponized malware' (Knapp and Langill, 2014; Vega et al., 2017) and Kim Zetter's infamous depiction of Stuxnet as 'the World's First Digital Weapon' (2014).

In the years leading up to the Operation Olympic Games, the planning and execution of was allegedly motivated by a desire to stall the Iranian nuclear programme. The U.S. considered it a vital strategic goal to slow down or halt Iran's means of uranium enrichment for nuclear power because they feared it was a gateway to the rearmament of nuclear weapons. Bearing in mind the U.S. offensive in Iraq in the 1990s and 2000s, using conventional military force was considered politically untenable (Sanger, 2012). At the same time, pressure from Israel to strike the Natanz facility to stop the enrichment of uranium was increasing (Sanger, 2018, p. 39; Lindsay, 2013). Inaction was reported to be considered unacceptable by the U.S. government, and the Bush administration saw two rather unfavourable options. The first was to support Israel should they opt to use conventional military force. The second was to continue the diplomatic track aimed at negotiating a deal with Iran. Alas, the second option might not adequately reassure Israel, and in the case of failure, potentially grant Iran leeway to further expand nuclear activities. Bush allegedly told his staff that he was in dire need of a third option. The U.S. Strategic Command presented him with the idea of a cyber operation. This was the beginning of Operation Olympic Games, which materialised as a seemingly plausible response to the quandary between the U.S./Israel and Iran (Sanger, 2018; Zetter, 2014).[30]

The operation was carefully planned over several years under the Bush administration. It was recognised by the U.S. National Security Agency (NSA), U.S. Cyber Command (USCYBERCOM) and the Israeli Unit-8200. The Central Intelligence Agency (CIA) had the overall operational responsibility (Sanger, 2018, p. 27, 174; Zetter, 2014). Following years of elaborate simulations and planning, the Stuxnet malware was delivered to the industrial control system's SCADA (supervisory control and data acquisition) sensors operating the enrichment centrifuges at the Natanz facility. The malware manipulated the rotation frequency of the enrichment centrifuges which over time caused the metal in the centrifuges to shake out of control and eventually split into pieces. During the destruction, operators at Natanz were presented with outdated centrifuge sensor data from recordings that had been carried out weeks before. This meant that the operators observed centrifuge settings that were seemingly normal. Because of the malware's ability to simulate and display incorrect data in the control room, the management at Natanz was convinced that the damage was caused by human error (Sanger, 2012, p. 169, 177). It is estimated that Stuxnet caused the destruction of over a thousand centrifuges (Albright et al., 2010; Vega et al., 2017, p. 157).

---

[30] One of the few available resources on Operation Olympic Games is the New York Times journalist David Sanger's book Confront and Conceal (2012). The book reveals through investigative journalism the sequence of events, supported by interviews with American government personnel who took part in the operation. Kim Zetter's book Countdown to Zero Day (2012) is an additional resource that patches together the publicly available technical details and accounts of the Stuxnet malware.

In the wake of Stuxnet, remedies against cyberattacks and the development of offensive cyber capabilities have been claimed to have become important priorities for the Iranian security services (Libicki, 2012, 2019; Segal, 2016). According to these perspectives, this enabled them to conduct major cyber operations – a cyber 'arms race' had seemingly begun. Less than two years after the Iranians fully understood the extent of sabotage at the Natanz facility in 2012, they deployed a wiper malware commonly known as Shamoon. The main target of the attack was the Saudi Arabian state petroleum company Saudi Aramco. The malware contained an overwriting component that compromised and destroyed data on more than 35,000 Saudi Aramco computers (Buchanan, 2020, pp. 149–151). In 2012 and 2013, Iran carried out a coordinated denial-of-service attack against several American financial institutions, causing them to lose the ability to maintain regular service operations. The operation became known as Ababil. It has been described as a response to U.S. economic sanctions against Iran (Council on Foreign Relations, n.d., b), but also as a direct reaction to Stuxnet (see Libicki, 2019). These different ideas about the reason behind deploying Ababil is yet another illustration that underscores the importance of understanding cyber operations in light of available and public knowledge rather than restricted to the cyber 'domain' as a retaliatory 'weapon'.

Despite the setback caused by Stuxnet, Iran's nuclear programme continued to grow steadily from 2013. While the Obama administration sought to negotiate with Iran to stall further development, the casino mogul Sheldon Alderson made a public statement that the U.S. should avoid negotiating with Iran altogether and go ahead and bomb its nuclear power plants. Iran was quick to respond. Within months Iranian operators carried out an attack on Alderson's company Sands Corp which resulted in the company suffering substantial financial losses. The attack has also been interpreted as politically motivated by Iran's desire to demonstrate equivalent cyber capabilities on a par with those of the Americans (Buchanan, 2017, pp. 82–84). The story of Stuxnet, however, cannot be understood without considering how unique and exceptional Operation Olympic Games was presented to be. The process of its planning and implementation was immensely resource-intensive and took several years. It was, however, undoubtedly thought of as being subject to a trade-off between speed versus intensity and control (Maschmeyer, 2022). Although the operation was organised by actors with offensive cyber capabilities, it has not prevented other states from entertaining different and more aggressive approaches to offensive cyber operations since. Iran's changes in security policy dispositions and the launching of offensive cyber operations against the U.S. and Israel is illustrative. The paradigmatic shift spurred by Stuxnet is indeed a nod to the development of an imaginary of 'strategic relevance' and utility of cyber operations.

As mentioned, Stuxnet has been described by the U.S. as an attack intended to prevent unnecessary escalation and bring Iran to the negotiating table to stall the potential future of its nuclear programme. When considered within frameworks of escalation dynamics, the operation has been said to have had a stabilising effect on the escalation level in accordance with the concept of pressure-release since conventional military force was assumed a viable alternative (Healey and Jervis, 2020). However, the question of whether the operation had a stabilising effect is not relevant unless considered in light of the imagined utility of cyber operations and available capabilities. The way cybersecurity threats were imagined changed in the wake of Stuxnet and had tangible consequences for how other states, now in addition to the U.S. and Israel, prioritised both proactive and pre-emptive security policies. This is illustrated by how U.S. government officials applied terminology in the public that spurred on an existential cyber threat such as 'cyber Pearl Harbor' in the wake of Stuxnet. Although the U.S. and the coalition with Israel were themselves in possession of capabilities to conduct serious cyber operations, government officials and Western media outlets produced a threat discourse that spread across the globe causing an upsurge in budgets for defence spending and investments in cyber capabilities. New vulnerabilities were discovered as potential existential threats, including industrial control systems such as the SCADA compromised by Stuxnet (Zetter, 2014).

The historical developments bear witness to the gradual normalisation of new risk associated with the functionality and resilience of modern industrialised societies and critical infrastructures, thus becoming inseparable from potential vulnerabilities. This led to a significant shift in how states and private companies, but also system engineers and administrators, dealt with network security and system management. However, as I return to later, imaginaries of cyber threats have since changed, and the focus has shifted towards so-called subversion operations, including information warfare campaigns and cybercrime. First, the next part, Section 6.4 delves into how Stuxnet was the catalysing event for the belief that cyber operations can function as substitutions to diplomacy and military force, and how these conceptions play into the emergence of 'strategic relevance' in political and strategic discourse.

6.4 Understanding cyber operations as substitutions

The strategic relevance of cyber operations is linked to their imagined utility as instruments of power. How states are considered to be using their potential to function as a substitute to a direct way of exerting power – conventional military force – is thus important for exploring how 'strategic relevance' emerges in the first place. The conditions conducive to substitution are also important for grappling with these perceptions as the social and material underpinnings of discourse that legitimise the use of cyber capabilities. The distinct academic claims highlighted in this section are worth exploring as the cornerstone to the policy development that was made possible after Stuxnet. These theoretical claims as drivers of knowledge production about threat tell the story of how strategic utility becomes a matter of fact.

According to dominant strategic and security studies scholarship, Stuxnet *did* function as a substitute for the U.S. government. The history of cyberattacks that have occurred since in the US/Israel-Iran dyad are also considered to belong to this category. Beyond the attacks that can be seen in direct relation to Stuxnet, the following decade was characterised by a series of cyber operations between the respective states (Schulze et al., 2020). The number of publicly known and/or attributed operations exceeded fifty as per the beginning of 2022 according to a mapping conducted the same year. The table below describes the most serious publicly recognised cyberattacks that occurred after Stuxnet.

Responsible actor	Victim	Year	Target	Result
United States and Israel	Iran	2010	Natanz facility	1,000 centrifuges destroyed, delays in technological development
Iran	Saudi-Arabia	2012	Saudi Aramco	Destruction of large amounts of data
Iran	USA	2012-2013	U.S. banks	Limited functionality in financial services
Iran	USA	2013	Sands Casino	Closing of casino, financial losses
USA	Iran	2019	The Iranian Defense Forces	Information security breaches in missile control system
Iran	USA	2019	American government institutions and critical infrastructure	Breach of information security
Iran	Israel	2020	Israeli water irrigation systems	Risk of chlorine poisoning and loss of irrigation system
Israel	Iran	2020	Shahid Rajaee Port	Loss of functionality in computer systems, delays in supplies
Israel	Iran	2021	Natanz facility	Centrifuges destroyed

Table 6.1: Destructive cyber operations by Iran, Israel, and the United States (2010-2022) (data from Vega, Bose and Buyuktosunoglu, 2017 and Barnes and Gibbons-Neff, 2019).

The attacks that were publicly acknowledged two to three years after 2010 have been publicly communicated as direct reactions to Stuxnet. Stuxnet has thus also been perceived as a starting point for a long-term state of ‘tit-for-tat’ in the isolated cyber domain, because the attacks were considered neither to escalate nor de-escalate conflict (Schulze et al., 2020). A similar episode that has underpinned the idea that cyber operations are a feasible alternative to diplomacy and conventional military attacks occurred when the U.S. attacked the Iranian armed forces' missile systems in 2019. The operation was seemingly intended to retaliate Iran's apparent role in attacks on oil tankers and an American drone. After only weeks of planning, USCYBERCOM carried out several counterattacks on Iranian intelligence and missile control systems. The attacks occurred on the same day as U.S. President Donald Trump rejected using conventional military force against Iran. The operation was allegedly authorised for the purpose of launching an attack below the threshold of armed conflict (Barnes and Gibbons-Neff, 2019). This decision has substantiated the notion that the operation may have had a stabilising effect on the escalation level. In accordance with the concept of pressure-release in view of the rational actor model, the cyber operation was deployed as a substitute for military force (Barnes and Gibbons-Neff, 2019; Healey and Singh, 2022).

If seen as isolated incidents, the rearmament of cyber capabilities and the many cyberattacks carried out in the decade after Stuxnet would indicate escalation between the US/Israel and Iran. The counterattacks carried out by Iran in the aftermath of Stuxnet suggest that Iran upscaled offensive cyber capabilities to compete with the U.S. and Israel through a large-scale initiative that included the development and deployment of weaponised malware (Segal, 2016; Healey and Singh, 2022). Shamoon, Ababil and the other operations presented in Table 1 have been understood in light of this rearmament (Libicki and Tkacheva, 2021). However, as argued, it does not make sense to view cyberattacks independent of a political, social and historically contingent context. To further explicate this point, which is notably subscribed to in predominant strategic studies scholarship, another way that the role of cyber operations has made its mark surfaces when returning to Herman Kahn's observation that non-kinetic adversarial activity can be described as 'subcrisis manoeuvring' (Kahn, 1965). Simply put, these are actions that are understood to take place at a lower level of conflict and do not necessarily contribute to escalation. If cyber operations are assessed in the context of the wider dynamics of conflict, they cannot be presumed to be escalating or de-escalating in and of themselves on an escalatory ladder (Schulze et al., 2020; Libicki, 2020).

In view of the history of the dyad in the aftermath of Stuxnet as shown in Table 1, known cyberattacks have varied in severity but not followed a classic ladder of escalation.

On the contrary, it has been argued instead that Stuxnet helped to bring the Iranians to the negotiating table with the U.S. and the P5+1 (Zetter, 2014; Sanger, 2018).[31] From this point of view, the Iranians seemingly understood how far the U.S. and Israel were willing to go to stall their means of uranium enrichment, and could have seen it as an opportunity to use it as a bargaining chip at the time. When the negotiations eventually took place, and the Joint Comprehensive Plan of Action was signed in 2015, the third option that former U.S. Presidents Bush and Obama sought has been said to have contributed to fulfilling their strategic goal of preventing Iran from developing nuclear weapons (see Sanger, 2018, p. 42). Since the operation has been foregrounded as an example of a form of statecraft that proved a successful alternative to diplomacy and conventional military force, it has played an integral part in the ideas that Operation Olympic Games was a turning point. This has been important for the promotion of the idea that offensive cyber capabilities are strategically relevant and an imagined instrument of power. Interpretations of substitutes for conventional military force have thus supported the establishment of the concept of pressure-release as it was observed in the case of Stuxnet and later in the 2019 attack authorised by Trump against Iran.

There is without doubt a clear discrepancy between the ‘predictions’ made about the utility of cyber operations – not to mention the dreaded outbreak of a ‘cyber war’ (Rid, 2013) – and what has transpired in the decade following Stuxnet. Inevitably, the way in which cyber operations have been deemed strategically (ir)relevant does not relate to whether retaliatory attacks fit into a classic ladder of escalation. The relationship between scholarly claims to strategic utility discussed above and subsequent analytical claims made constitute the basis for political action. That is, discursive claims in theoretical debates about the role and meaning of cyber operations and their effects are deeply inscribed into ensuing policymaking and responses in situations of conflict. The next and final part, Section 6.5 teases out the manner in which Stuxnet ‘popularised’ cyber doom scenarios, state exhibitionism and discursive development of cyber capabilities as strategic and political choices, largely driven by authority statements, industry investments and subsequent threat inflation.

[31] The P5+1 are the permanent members of the UN Security Council and Germany.

6.5 The golden age of cyber war – and back

Although there can be no doubt about the increase in the number of small and large-scale cyberattacks and operations organised among state and non-state actors since the early 2000s, the use of cyber operations in international conflict is indeed far less severe than the gloomy predictions made in the immediate aftermath of Stuxnet. Admittedly, Stuxnet was the first known cyber operation to cause physical damage, followed by widely known operations such as the attacks on the Ukrainian power grid in 2015 and 2016, the U.S. Colonial Pipeline in 2021, and the attack on the Viasat satellite functions in the early days of the Russian invasion of Ukraine in 2022.[32] But the subsequent inquisitiveness that fuelled not only debates on how to conquer this 'new' threat but also strengthen national and international security strategies demands further attention. Stuxnet is an ample illustration of a significant epistemic turning point, meaning knowledge interactions that enabled the emergence of an ostensible 'existential threat', in turn producing imaginaries of strategic relevance in a domain subject to ambiguity relating to what threatens, and thus security *for whom*, *by whom*, and for *what purpose* (Lawson and Middleton, 2019; Sandvik, 2016, pp. 177–176). The ambiguity surrounding knowledge of cyber operations and threat perception seen either in isolation or in broader international political contexts carries significant impact moulded on its imagined role as substitute for conventional military force.

The damage caused by Stuxnet remains a decisive turning point that transformed the way technical vulnerabilities were imagined and discussed among politicians, industry, military and IT security communities, as well as in research and popular culture from the 2000s onwards. Many feared that the Stuxnet malware code could 'spread' uninhibitedly among actors with malicious intent (Lindsay, 2013, pp. 366). Doomsday scenarios were particularly popular in the American media and among politicians, including speculations

[32] Cyberattacks that either directly or indirectly causes physical damage are considered kinetic cyberattacks (Applegate, 2013). In December 2015 and again in 2016, Ukraine's power grid was hacked by actors who disabled the control systems, leaving large parts of the country without power for several hours. The attack was the first known case of a cyberattack causing power outages (Kostyuk and Zhukov, 2017). In 2021, a network attack on Colonial Pipeline forced the company to shut down pipelines transporting gasoline to the US east coast (Walsh, 2021). A cyberattack on the infrastructure of the satellite KA-SAT, owned by Viasat, disabled the Internet connection of thousands of people across Europe in addition to parts of the Ukraine army communication infrastructure (Burgess, 2022).

about the looming ‘cyber Pearl Harbour’ and the destruction of the critical functions of society by complex cyber operations (Lawson and Middleton, 2019; Lawson, 2013). Former U.S. Secretary of Defence and CIA Director Leon Panetta stated that cyberwarfare was on the rise and that the U.S. could expect an attack on a par with 9/11. Barack Obama wrote in 2012 that the risk of cyberattacks against the U.S. was considered one of the greatest threats to national security (Lindsay, 2013, p. 367). Some went as far as comparing cyber ‘weapons’ to atomic bombs (*The Economist*, 2010, p. 11). However, as mentioned, no such developments have thus far happened. While this does not mean that the problems posed by the continuous digitalisation of infrastructures do not exist, these problems are far less remarkable or extraordinary than these essentialist accounts of cyber operations claim. Instead, these accounts are historically and politically situated and change according to the current trends of new and emerging technologies.

The essentialist beliefs in the risk and threat posed by so-called kinetic cyberattacks has not matured as expected in accordance with their predictions, including those who ascribe cyber operations to the economic and political ‘laws’ of structural power balances (Nye, 2011; Valeriano and Maness, 2018). For instance, the concern that Stuxnet bestowed other actors with code that could instruct similar malicious attacks was misleading because the code itself did not provide additional infiltration guidelines to those previously discovered in malware such as Conficker.[33] In addition, the Stuxnet payload was specifically coded to target only the SCADA (supervisory control and data acquisition) system at the Natanz facility, meaning the malware was not directly useful for other purposes (Lindsay, 2013, p. 388). What can be gathered from Figure 6.1 below is that the most important turning point for the dominant – and particularly American – view on cyberthreats was the U.S. presidential election in 2016. To them, Russian information operations demonstrated a different type of offensive cyber capability that attempted to interfere with democratic processes. Focusing on the possibility of a ‘cyber Pearl Harbor’ while Russia struck to assert political influence through information channels was a critical moment at odds with the previously confined role of cyber operations (Lawson and Middleton, 2019, pp. 1-2).

[33] Conficker was a malware that spread to millions of computers around the world before it was discovered in 2008. The goal was to exploit weaknesses on computers running Microsoft operating systems.

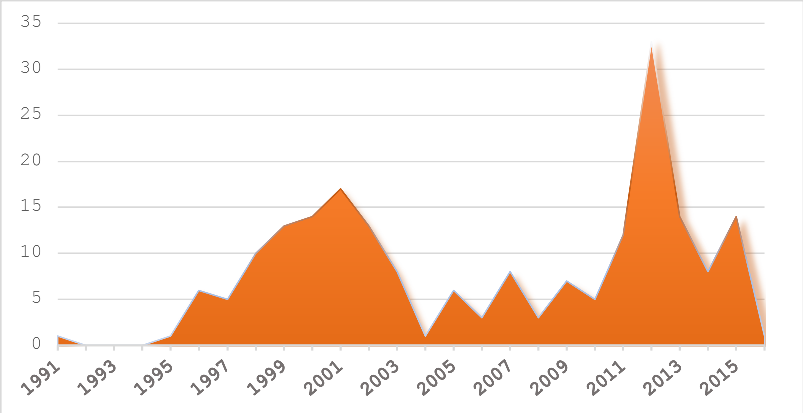

Figure 6.1: Mentions of cyber Pearl Harbor in major U.S newspapers, 1991-2015 (from Lawson and Middleton, 2019, p. 12).

Max Smeets and Stefan Soesanto (2020) illustrate a similar trend within research that is consistent with the discourse on cyber revolution and other doomsday scenarios. ‘Cyber war’ had its golden age in cybersecurity research shortly after Stuxnet. After 2016, it became abruptly less popular to analyse deterrence strategies in the cyber domain. It may very well be that the preceding notion of cyberthreats as mainly kinetic security threats was refuted when the U.S. had to deal with Russian interference during the 2016 election. This transition meant that both politicians and scholars alike had to alter their understanding of offensive cyber operations.

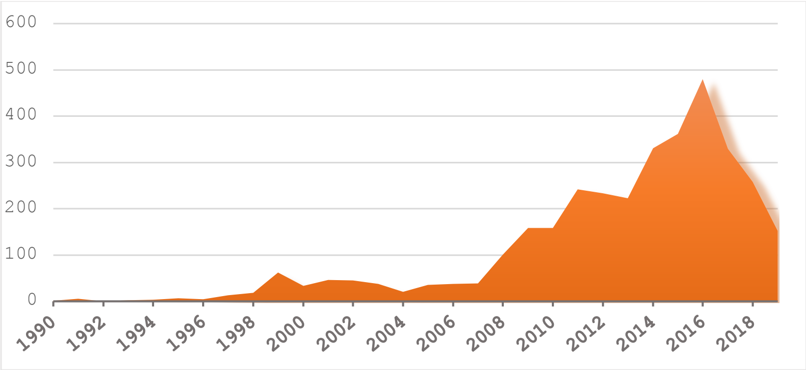

Figure 6.2: Journal articles, book chapters, and research reports on cyber deterrence, Jan 1990–Jan 2020 (from Smeets and Soesanto, 2020).

The expansion of common beliefs to a wider range of possible manoeuvres in the cyber 'domain' illustrates why research on security and IR should not fail to consider cyber operations as historically situated and discursively produced in accordance with securitisation theory (Buzan et al., 1998). This helps us better comprehend the challenge scholars face in trying to fit offensive cyber operations into existing frameworks to grapple with deterrence and escalation in international conflict.

Stuxnet is time and again referred to as 'the World's First Digital Weapon' (Zetter, 2014). However, as canonised by Thomas Rid, 'cyber war will not take place' (Rid, 2013). Stuxnet did not catalyse a cyber revolution, and a 'cyber Pearl Harbor' is yet to occur. When Stuxnet signalled that cyberattacks can indeed sabotage systems and cause damage, subsequently feeding into the idea that it could be categorised as a substitute for conventional military force (Lindsay, 2013, p. 402). This could indeed have been the alternative President Bush allegedly hoped for when the U.S. sought to curb Iran's nuclear activities without escalating conflict. But that does not mean that cyber operations can be understood as a substitute in and of themselves. Rather, it shows the importance of considering how imaginaries of cyber operations as means to strategic ends rely on the extent of knowledge about them and the material capabilities available to know the threat in the first place (Dunn Cavelty, 2018; Stevens, 2020). Returning to Figures 6.1 and 6.2 shows how engagement with cyber-related topics is interlinked with the willingness to do so. As argued by Myriam Dunn Cavelty:

> Beyond the question of whether there is an *objective* increase in willingness and skill for cyberattacks among political actors, the focus of research on SCADA systems (as targeted by Stuxnet) and on the infrastructure considered the most 'critical' for society (electricity) is intertwined with political interests and sensibilities. (2018, p. 25, *italics in original*).

The material realities of discovering Operation Olympic Games following the forensic analyses of Stuxnet conducted by Symantec (Langner, 2011) formed the basis for subsequent political action (Balzacq and Dunn Cavelty, 2016; Stevens, 2020). As Stevens (2020) argues, "reports such as Symantec's are an important constitutive element in wider practices of hardening facts about threats" and technical reports on cyber operations are "loaded with political, instrumental, and strategic choices" (Stevens, 2020, p. 131). Thus, adding to the impact Stuxnet had on orthodox security scholarship on cyber operations, it was not only productive in creating a space for 'new' knowledge about threat, but also the conceptions of 'risk' and political strategies for deterrence and political coercion below the threshold of armed conflict. Stuxnet was also the harbinger of modern cyber *defence*, forming the basis for today's engineering of intrusion detection and prevention mechanisms for critical infrastructure (Dunn Cavelty, 2018). Before Stuxnet, there was a common belief that industrial control systems did not need significant safeguarding since the software was not considered a relevant target for threat actors (Karnouskos, 2011; Knapp and Langill, 2014; Buchanan, 2020). Forensic reports on Stuxnet reinforced practices aimed at 'built-in' security measures with the ambition to pre-empt attempts to sabotage even air-gapped systems (Vega et al., 2017).

The paradigmatic shift in the way offensive and defensive cyber is conducted and how it is made known is owed to the assembly of actors, technical means and knowledge that emerges in union. The point being made is that contextual elements play into how cyber operations are situated, and thus understood, creating the conditions for its presumed strategic relevance. This is where strategic studies scholarship falls short by taking for granted the 'laws' of structural power balances, in turn asserting a premise for analyses. How cyber capabilities are deployed in times of conflict or politically-strained relations does not simply rely on the political history and context but the means available to analyse, comprehend and use cyber capabilities. Even as IR and Strategic Studies scholar Jon Lindsay argues, Stuxnet 'had more influence on our understanding of cyber warfare than cyber warfare ever had on Iranian enrichment' (Lindsay, 2021). The interplay between knowledge and technical capabilities continuously produces ideas about what threatens, against whom, and the subsequent constitutive effects of ‘cyber’ on politics and international security.

6.6 Conclusion

This chapter has argued that Stuxnet and its aftermath can be understood to have spurred on a paradigm shift for discourses on the strategic utility of cyber capabilities and operations. A critical review of the trajectory of academic literature, largely driven by Strategic Studies scholarship, has shown that the idea of ‘strategic relevance’ is partly produced by discursive claims to the utility of cyber operations as instruments of power. The literature, when viewed in relation to political claims and developments in security dispositions, refers to a tangible empirical record that purports to have solved the problem of how to understand cyber operations as means to strategic ends. This includes, as discussed in this chapter, whether cyber operations function as a substitute somewhere between diplomatic means and conventional military force or as a mechanism of pressure-release. I have thus shown that the paradigm shift is inevitably manifested in material-discursive knowledge practices. Stuxnet highlighted that the capacity to act is not merely a causal effect of (de)escalation dynamics. Instead, in accordance with securitisation theory, the capacity to act is enabled and constrained by the discursive processes and material means available to envisage cyber offence and defence. Stuxnet illustrates a significant epistemic turning point – knowledge interactions that have recognised and stabilised the emergence of an ‘existential threat’ – which has in turn produced, and continues to produce, the meaning of ‘strategic relevance’ of cyber operations.

The aim has by no means been to measure the strategic (ir)relevance of cyber operations. Rather, this chapter has pointed to the importance of considering the linkages often ignored in traditional security studies, namely how the exceptional story of Operation Olympic Games and the Stuxnet malware has underpinned the way contemporary understandings of the (potential) role of cyber operations in international conflict prevail. The imaginative role of cyber operations and capabilities as strategically relevant continue to influence the way cyber capabilities are understood and deployed in the context of policy and international security. Revisiting Stuxnet (again) has shed light on the story of how the understandings of cyber capabilities are produced, historically, discursively and, *inter alia*, materially. With this in mind, scholars across the spectrum of security studies under the IR umbrella can take on the discovery of ‘new’ security threats and capabilities without losing sight of the contextual and situated accounts that produce the meaning of ‘relevance’ in the first place.