Restraint under conditions of uncertainty: why the United States tolerates cyberattacks

Kaminska, M.K.

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2021, 1–15
doi: 10.1093/cybsec/tyab008
Research Paper

Research Paper

Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks

Monica Kaminska [1,2,*]

[1]Hague Program for Cyber Norms, Institute of Security and Global Affairs, Leiden University, Wijnhaven, Turfmarkt 99, 2511DP The Hague, The Netherlands and [2]Department of Politics and International Relations, University of Oxford, Manor Road Building, Manor Road, Oxford OX1 3UQ, UK

*Correspondence address. Institute of Security and Global Affairs, Leiden University, Wijnhaven, Turfmarkt 99, 2511DP The Hague, The Netherlands. Tel: +31 70 800 9512; E-mail: m.k.kaminska@fgga.leidenuniv.nl

Received 2 July 2020; revised 21 December 2020; accepted 15 February 2021

Abstract

The United States struggles to impose meaningful costs for destructive or disruptive cyber operations. This article argues that the United States' restrained responses stem from a desire to avoid risk in an inherently uncertain operational environment. The societal desire for risk avoidance is the prism through which policymakers address the cyber domain and deliberate responses to attacks. The article shows that two particular operational characteristics of cyberspace—its complex adaptiveness and the ease of proliferation—combine to increase the risk of misattribution and the risk of unintended effects, including collateral damage, inadvertent escalation and blowback. These characteristics present a particular obstacle for risk societies such as the United States in the application of meaningful punishments. In addition to establishing the roots of US restraint, the article traces the application of risk management practices, including preventive action, increasing resilience and consequence management, from the Obama administration to the Trump administration. The analysis reveals that risk management has underpinned the overall US approach to the cyber domain.

Key words: strategy; risk; deterrence; escalation

Introduction

When the United States falls victim to major cyberattacks, it faces a punishment problem: despite formally subscribing to a strategy of deterrence,[1] it struggles to meaningfully respond to cyber operations whose effects are destructive or disruptive. The unwillingness to issue meaningful responses has eroded among adversaries the expectation of reprisal for such attacks, which increases the probability that the operations will continue to grow in number. As the Cyberspace Solarium Commission, established by US Congress to explore, among other things, the response problem, noted, 'Today most cyber actors feel undeterred, if not emboldened, to target our personal data and public infrastructure. … [T]hrough our inability or unwillingness to identify and punish our cyber adversaries, we are signalling that interfering in American elections or stealing billions in U.S. intellectual property is acceptable' [3]. If new strategies are to avoid similar failures of implementation, then it is important to understand the socio-cultural and material roots of this restraint.

The term 'meaningful punishment' entails the imposition of 'swift, costly, and transparent consequences' to 'deter future bad behavior,' as stated in the US National Cyber Strategy [1]. Meaningful punishment is essential to establish that the state in question has the credible will and capability to respond to attacks in the future [4].

[1] The United States has stated that it will pursue not only 'deterrence by denial', or 'efforts [that] aim to persuade adversaries that the United States can thwart malicious cyber activity', but crucially also 'deterrence by cost imposition', or 'measures [that] are designed to both threaten and carry out actions to inflict penalties and costs against adversaries that choose to conduct cyber attacks or other malicious cyber activity against the United States'.

The imposition of meaningful punishment, however, does not necessarily entail the objective of influencing the adversary to abandon their future offensive plans altogether—or absolute deterrence. As Thomas Rid noted, absolute deterrence was a rare Cold War exception owing to the nature of nuclear weapons [5]. Rather, meaningful punishment is meant to affect an adversary such that they will restrain or otherwise modify their actions in order to moderate or avoid a future punishment [5].

Thomas Schelling offered an additional elaboration on how to communicate with an adversary through meaningful punishment. He argued that the 'idiom of reprisal' is only effective when there is a connection between an action and a reprisal. He therefore recommended that actions should be part of a 'coherent pattern'; a response should be mounted in the same 'currency' or 'language,' and the enemy should be able to clearly determine that the punitive measures implemented are a form of reprisal as opposed to opportunistic assault [6]. In other words, in order for a punishment to be effective, it has to communicate a clear message by means of its intensity and specificity. To fulfil Schelling's 'currency' criterion, it would therefore seem that the United States should elect to respond to a cyber attack with a digital assault of its own. There is little doubt that the United States possesses the capabilities required to do this.[2]

This article argues that the reason the United States fails not only to respond in kind,[3] but also fails to respond with meaningful cross-domain punishments, is rooted in the dominant risk paradigm that guides the US approach to international cybersecurity. The cyber domain's high level of uncertainty—inordinate even by the standards of international anarchy—is especially problematic for risk-averse states like the United States and underpins an attitude of restraint following an attack. Based on the work of sociologists [11, 12], 'risk societies' are those that, as a result of historical and cultural factors, exhibit a strong societal preoccupation with the negative side effects of industrialization and modernization [13]. They find the uncertainty and incalculability of future dangers that result from technological advancement highly daunting. Policymaking in risk societies is guided by the desire to either avoid or minimize future hazards and dangers and an intense, even anxietal, focus on public safety [14].

Unlike states with a higher tolerance for risk, risk societies will see the technical features of the cyber operational environment that create unpredictability and uncertainty as an obstacle to meaningful punishment. Two characteristics are especially important. One is the complex and adaptive nature of the domain. It features unclear feedback loops, multiple control parameters and indirect information sources [15]. The potential for unintended effects and system accidents is therefore great [15, 16]. The second important feature is proliferation: the emulation and re-use of cyber capabilities by actors other than their creator [17]. The relative ease of capability proliferation in cyberspace has meant that weaker states and even criminal groups are able to launch destructive attacks with global ramifications.

These features of the operational environment have two important implications for states seeking to respond to cyberattacks. First, operational ambiguities introduce the risk of misattribution of attacks. This means that in order to achieve what a risk society considers to be a satisfactory level of confidence in the perpetrator's identity, the process of attribution will be lengthy, even to the point where a meaningful response might no longer be viable. Second, the complexity and high degree of interconnectedness between computer systems and networks means that in addition to introducing problems of interpretation of the initial attack (victims find it hard to determine the perpetrator's intent from the effects of the operation), risk-averse responders may be reluctant to engage in cyber retaliation for fear of malware spreading to unintended targets and causing collateral damage, 'blowback' or escalation. States with a high dependency on Internet-connected infrastructure and systems, which have often been developed with scant attention to security, are particularly vulnerable to cyber escalation and blowback [18].

While the risks created by operational features will in reality affect all highly networked states equally, risk societies like the United States, as a result of a low societal appetite for risk and a fear of uncertainty, will perceive them as a particular obstacle to meaningful responses. Concerns about risk will inform the response calculus, leading, in the case of the United States, to the selection of weak responses such as limited economic and diplomatic sanctions and indictments or no response at all. In addition to being unwilling to engage in tit-for-tat cyber exchanges, risk societies will seek to address the national security implications of the operational environment through risk management practices. These practices, however, should not be understood as a response to individual cyberattacks that substitute for punishment. They are not intended to influence the resolve of the attacker to engage in attacks, but rather are employed by risk societies to mitigate as much as possible the scale and effects of operations on digital infrastructures, while maintaining an awareness that complete security is unattainable.

While the United States, as a result of a combination of societal, historical and cultural factors,[4] is wary of risk and uncertainty and therefore reluctant to respond meaningfully, some of its adversaries seem to take a different approach. Iran is an example of a state that has become particularly adept at cyber retaliation. A leaked NSA document reveals that the Agency interpreted Iran's 2011–2013 attacks on the US financial sector as retaliation for 'Western activities against Iran's nuclear sector,' which presumably included the Stuxnet cyber operation. Iran's highly destructive cyberattack on Saudi Aramco of August 2012 was likewise seen by the NSA as punishment for a similar cyber operation against Iran's oil sector in April 2012 [20].

The remainder of the article has six sections. The first section illustrates the puzzle presented by the lack of meaningful US responses to cyberattacks. The second section introduces risk management as the theoretical lens through which the restrained responses of the United States can be understood. The third section outlines the two key operational characteristics of the cyber domain,

[2] For example, the United States consistently leads in international cyber power rankings. See: [7–9].

[3] It is possible that US responses to cyber incidents have been covert and therefore have not entered into public knowledge. There are two important caveats to this observation. First, the interconnectedness of systems in the cyber domain means that there is a high degree of probability that malware would end up spreading outside its intended target. If this is the case, the operation is likely to be picked up by threat intelligence companies, which regularly survey the landscape for new strands of malware and report publicly on their findings. In other words, a significant cyber response would most likely enter into public knowledge, much like Stuxnet did. Secondly, there is a strong argument that responses that are public are more meaningful. This is particularly the case if a victim has attributed an incident publicly and promised to follow-up with consequences. Should it fail to do so, it then faces reputational costs in terms of appearing weak in the eyes of the international community. For further elaboration of this point, see [10].

[4] For a detailed historical discussion of the emergence of the risk society in the United States, see [14, 19].

complex adaptiveness and proliferation of capabilities, which, as the fourth section explains, contribute to the creation of uncertainty by introducing the risk of misattribution and the risk of unintended effects. These two sets of risks lie at the heart of the response dilemma for risk societies when they find themselves unable to achieve attribution of a satisfactory quality in the time they have to respond meaningfully and are unable to issue a response in kind for fear of triggering unintended effects. The fifth section analyses evolving US risk management approaches to cyber conflict from the Obama administration to the Trump administration. The article concludes with a recommendation for further scholarly examination of the implications of proactive risk management in terms of the normalization of forward-leaning preventive practices in the cyber domain.

The puzzle of restrained responses

American policymakers have vehemently decried the damaging effects of major cyberattacks. They have issued public attribution statements promising to inflict costs on attackers, yet have rarely followed-up with meaningful forms of punishment.[5]

A case in point was the US reaction to the 2017 NotPetya attack. Although the attack was directed at Ukrainian companies and institutions, its low degree of customization in target selection meant that it spread much further and disrupted organizations across the globe, including shipping companies,pharmaceutical corporations and hospitals in the United States [22]. Attributing the operation to Russia, the US government described the attack as the most destructive one in history [23]. Its monetary effects alone were estimated at 10 billion dollars. The shipping company Maersk revealed that it had to reinstall its entire IT infrastructure in the attack's aftermath [22, 24]. The operation also had a significant financial impact on FedEx and Merck [24, 25].

After delivering an internationally coordinated statement of public attribution—which included a promise that the 'reckless and indiscriminate cyber attack' would be 'met with international consequences' [23] – the United States levied financial sanctions against 5 Russian entities and 19 individuals. The measures, however, were part of a blanket sanctions package that was designed to counter a number of other actions, including election interference, hacks of Yahoo and attempted intrusions into the electrical grid [26]. The sanctions did not explicitly punish the offenders for NotPetya. Additionally, US congressmen pointed out that many of the sanction targets had already been penalized by the Obama administration, while others had been charged within the criminal justice system [26]. It is therefore surprising that a definitive statement of public attribution was followed by a vague and restrained reprisal.

Let us recall another incident: the Obama administration's reaction to Russia's interference in the 2016 US presidential elections, which took the form of hastily applied diplomatic and economic sanctions. In this case, it seems that policy elites were aware already at the time of deciding on the responses that their chosen punishments would not be meaningful.[6] In his memoirs, recounting the final weeks of President Barack Obama's time in office when the sanctions were announced, James Clapper, former Director of National Intelligence, wrote, 'I didn't think the response was commensurate with what they'd done to us, but I also knew we weren't prepared to take more drastic steps' [27]. Daniel Friend, who oversaw the US government's sanctions policy under Obama, disclosed: 'The Obama administration—in my view, and I was in it, OK? I was working on sanctions then—did not respond with adequate strength to the Russian interference in our elections ... What we did in December 2016 was a very light set of sanctions, which I feel were frankly inadequate ... those sanctions are not apt to be terribly effective, and we knew it. That was not enough'.[7] Another senior official in the administration commented: 'It is the hardest thing about my entire time in government to defend'. 'I feel like we sort of choked'.[8]

Upon taking office, the Trump administration's response to the election interference was no more muscular and, again, recognized as such by policy elites. In 2014, still as a nominee for the Commander of Cyber Command, Michael Rogers had told the Senate Armed Services Committee: 'I believe the U.S. may be considered an easier mark because our own processes and criteria lead the adversary to believe, rightly or wrongly, that we do not have the will to respond in a timely and proportionate manner, even when attribution is available' [30]. In 2018, Rogers, by then Director of the National Security Agency and Commander of Cyber Command, admitted to the same committee that Putin had paid 'little price' for interfering in the US election and therefore would continue to direct such activity. 'What I see on the Cyber Command side leads me to believe that if we don't change the dynamic here, that this is going to continue, and 2016 won't be viewed as isolated'. 'They haven't paid a price at least that's sufficient to get them to change their behaviour,' he affirmed.[9]

Although this article focuses on the United States, the country is not alone in its response dilemma. The UK has similarly showcased extraordinary levels of restraint in response to cyberattacks—also in spite of attributing these publicly. As an example, the WannaCry operation compromised the networks of the UK's National Health Service, affecting 80 hospital trusts and 595 general practitioner surgeries [32]. The attack resulted in a monetary cost of between 4 and 8 billion dollars globally and, in the UK, the cancellation of 20,000 hospital appointments and operations, with ambulances reportedly being diverted from Accident and Emergency Departments [22, 33]. In a statement after the attack, a Foreign Office minister described the operation as 'one of the most significant to hit the UK in terms of scale and disruption'. He promised that the UK would 'identify, pursue and respond to malicious cyber activity regardless of where it originates, imposing costs on those who attack us in cyberspace' [34]. Yet, as far as is known publicly, the UK's only response was an attribution statement and verbal condemnation of the attack.[10]

[5] This is particularly puzzling because 'All other things being equal, attribution raises the probability of punishment' [21].

[6] It should be noted that policymakers' public statements cannot always be taken at face value as these might serve strategic purposes. There is no sure way to completely eliminate this methodological issue, but it may be mitigated through corroboration of public statements with other data sources. Accordingly, the sentiments expressed by policymakers that are quoted in this article have been corroborated in personal interviews.

[7] Friend quoted in [28].

[8] Anonymous Senior Official quoted in [29].

[9] Rogers quoted in [31].

[10] This article deliberately does not discuss responses to Computer Network Exploitation (CNE) operations, that is, operations seeking to gather information, rather than manipulate or delete it [35]. The paper is interested in attacks that sought to disrupt, deny, degrade, destroy or influence [36]. It is the responses to these attacks, or lack of a response, that have been most stark and surprising in light of the official strategy of deterrence and repeated statements that these attacks would be met with cost imposition. Responses to China's cyber operations, which are primarily espionage-driven (for evidence of this point see [37]), therefore lie outside the scope of this research. This does not mean that cyber espionage operations are inconsequential. As Harknett and Smeets have

Roots of the puzzle: Risk aversion

The understanding of 'risk' here is based on the concept as put forward by sociologists Ulrich Beck and Anthony Giddens [40]. They argued that in the modern era, the 'darker side' of industrialization and globalization had facilitated the emergence of risk societies, societies preoccupied chiefly with preventing and minimizing the uncertain hazards created by these processes [13]. The main concern of a risk society is continuously trying to identify potential risk and intervene in time to avert disastrous consequences [41]. Risk societies are 'reflexive' in the sense that they have to contend with risks that are a by-product of their own actions and technological advancement [13]. Nowhere, perhaps, is this more starkly illustrated than in the cyber domain: the United States led the digital revolution and greatly benefited from it, hence its current high level of dependence on computer systems, but the trade-off of this modernization is a heightened vulnerability to its side effects [42]. In risk societies, an increased societal awareness of the negative side effects of industrialization and globalization creates in them a widespread anxiety about the uncertainty of future scenarios [43].

In contrast to Cold War-era threats, which were typically well-defined and elicited a clear reaction, the uncertainty of present security challenges and the consequent inability to make decisions based on calculations of causes and effects confounds societies with a low tolerance for risk [14, 43]. The management of present risks involves reducing the likelihoods of threatening scenarios to a level deemed tolerable or as low as one can reasonably achieve [14]. 'Risk thinking' is therefore characterized by policymakers considering policy options in terms of probabilistic future scenarios [44, 45]. Anticipating uncertain future events, thinking through decisions on the basis not of what happens but of what *might* happen, and introducing proactive measures to avert worst-case scenarios are all telltale signs of risk management campaigns [19, 44, 45]. One example of 'risk thinking' is the increasing application of the precautionary principle[11] to security decision-making to justify protective measures, pre-emptive or anticipatory action, in situations where there is 'a lack of evidence of harm or straightforward causal relationships' [14, 46].

Not every highly industrialized state is a risk society, however. A particularly important insight from Beck's work is that 'risk is inherently affected by politics and the culture of each state' [47]. Although material realities matter in framing the risk environment, the way in which they are perceived is subjective, meaning that different societies will have different risk thresholds [48]. Michael J. Williams advised looking at risks in terms of objective dangers and subjective, culturally constructed risks: a great white shark, for example, is objectively a danger, but the 'riskiness' of swimming with sharks is dependent on one's perception of the situation, which is culturally determined [49].

In placing emphasis on the incalculability of future risk and its subjective nature, the sociological stance on risk management departs from the one typically provided in the organizational and finance literature, whereby risk management involves *quantifying* the 'probability and severity of risks' so as to aid decisions on how to address them [50]. In other words, the risk society perspective believes that there is no single, objective way to assess risk as a function of threat (the likelihood that an asset is attacked), vulnerabilities (the likelihood of succumbing to that attack) and consequences (the likely adverse effects of an attack) [51] because these are informed not only by material realities but also by how concerned a society is with safety and which future scenarios it seeks to avoid.

Recent scholarly work by Sarah Kreps and Jacquelyn Schneider indicates that in the United States, there exists a societal awareness of America's asymmetric vulnerability in cyberspace. Using a survey study, the authors showed that US domestic public believe in a position of restraint in response to cyberattacks, and the reasons for this include 'the "desire not to escalate" and the fear that an aggressive response would create higher costs and "worsen the conflict"'—likely due to the fact that domestic publics see cyberspace as a qualitatively different domain [52].

The analysis below will show that the complex structure and technical characteristics of the cyber operational environment pose a particular challenge to states that are socially, culturally and historically conditioned to avoid and minimize risk—these states will pay more attention to the features that create unpredictability, including when responding to cyberattacks, than states with a higher societal tolerance for risk and uncertainty. States that put a premium on risk avoidance will focus most of their efforts on proactive defence and, if this fails, put in place strategies to curb the destructive potential of attacks. Drawing from the risk management literature, we can identify three main practices that risk societies are likely to carry out in an attempt to manage risk and uncertainty: preventive action, increasing resilience and consequence management. We now turn to a discussion of these practices.

Preventive action

Prevention in the cyber domain is the go-to practice for risk societies seeking to mitigate the risk of future attacks. Preventive action and the related, albeit definitionally separate, concept of pre-emption are often associated with the Bush Doctrine, reigniting debates about the United States' invasion of Iraq in 2003. The concept of preventive action, however, goes back at least far as Thucydides' account of the Peloponnesian War in the fifth-century BC when the Spartans reasoned that Athens had to be eliminated as a potential threat before it grew too powerful [53]. To make the concept of prevention more useful in a cyber context, we must first distinguish between prevention and pre-emption and secondly between a preventive war, a preventive strike and preventive action.

The distinction between preventive and pre-emptive strategies centres on timing: a pre-emptive strike takes place when an attack is credibly imminent [53, 54]. The defender is faced with a scenario of either striking first or being on the receiving end of an attack [54]. Scholars have argued that the so-called 'Bush Doctrine' was in fact a strategy of prevention, rather than pre-emption, as it emphatically claimed to be [53–56].

Estimating the immediacy of an attack is difficult and often subjective even in the physical domain, which has historically limited the usefulness of 'imminence' as a guide to action [53]. In the cyber domain, where signalling is impaired, and there are often no visible signs of attack preparation like troops amassing at borders, this is

argued, espionage campaigns, such as the ones directed by China, are *cumulatively consequential* in their impact on national sources of power [38]. Individual responses, however, are 'not flexible enough' to address their continuous nature [39] and, more generally, the extent to which such operations can be deterred is debatable.

[11] The most widely known definition of the principle comes from the 1992 Rio Declaration on Environment and Development: 'Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation' [46].

even more difficult. On top of the lack of warning, the attacks themselves take place within milliseconds. Pre-emption is therefore often not a viable strategy in the cyber domain. Prevention, however, can be viable.

Prevention is a strategy designed to eliminate potential threats or thwart the adversary's acquisition of threatening capabilities [53, 55]. Often, a preventor will act in order to stop an enemy from shifting the balance of power or engage in actions that would be intolerable to the preventor [54]. Prevention implies an unwillingness to put up with certain kinds of risk and an intention to control the external security environment [54]. Prevention therefore often involves a great deal of prediction of future threats amid uncertainty. It leaves far more choice for the defender than pre-emption, where it is the adversary that controls the timing having already decided to launch an attack [54].

A strategy of prevention in the physical domain carries significant risks due to the distinct difficulty in estimating the future gravity of threats in the international environment and the associated wide margin of error [54]. Additionally, both preventive strikes and a preventive war involve violence. A preventive strike is a short duration military action to remove an adversary's capability; this can be done through covert operations, interdictions or targeted killings [53]. A preventive war is an extended military engagement designed to defeat the enemy before the enemy has had the time to grow into a formidable threat to the preventor. In the case of preventive war, policymakers decide that it is better to fight 'today' than 'tomorrow,' when the enemy might be in a better position to alter the balance of power [54].

Unlike in the conventional military domain, in the cyber domain eliminating a potential threat can be achieved by non-violent actions such as taking an adversary's attack infrastructure offline or releasing information about exploits used by an adversary into the public domain. It also often involves operating in adversaries' networks, or so-called red space, and can result in some level of destruction, mostly of data. But it does not carry the same probability of violence or loss of life as in the physical domain. Thus, preventive *action* is a more accurate term for such activity in cyberspace. The US case study in section five will illustrate preventive action in the cyber domain.

Increasing resilience

Increasing resilience is defined as developing the capacity to 'withstand, recover from, and adapt to external shocks' [50]. For our purposes here, the most important feature of resilience-building is that it takes place *before* an incident has happened and includes technical measures that can reduce harm in an automated and pre-programmed manner. *After* an incident has taken place, states will seek to manage the attack's harmful consequences, which is a human-oriented effort because it involves analysis and decision-making during the event itself (as we will discuss next).

Examples of resilience-building in the cyber domain include the introduction of intrusion detection technologies, improving general cyber 'hygiene' through, for example, introducing two-factor authentication, conducting regular network penetration tests, installing 'patches', updating operating systems, maintaining robust backup procedures and, more generally, building systems that can withstand attacks [21, 57]. Some might argue that resilience-building (and also preventive action) are no different from the implementation of mechanisms for deterrence by denial [58].[12] Indeed, if robust defences of a target are known to the adversary, the techniques used in risk management may also serve deterrence purposes, that is, they may have the psychological effect of dissuading the adversary from launching an attack on that particular target in the first place [59].[13]

Consequence management

In cases where a cyber operation does succeed in breaching a system, states will engage in consequence management. Consequence management are actions taken during the course of or in the aftermath of an incident to reduce the impact of its effects and aid recovery [60]. While bolstering resilience intends to increase the security of systems to prevent cyberattacks from breaching them and, if that fails, trigger previously implemented measures that will allow for their quick restoration, consequence management is human-oriented: it involves decision-makers analysing and addressing an already ongoing cyberattack in such a way as to prevent further loss or, in the aftermath of an attack, alleviate damage. An example of consequence management is cooperation among government officials in different countries to disrupt foreign-based botnets during the course of an attack.

Sources of operational uncertainty in the cyber domain

Having discussed the risk framework, we can now ask what aspects of the cyber operational environment create uncertainties with policy consequences particularly for risk societies. There are two main characteristics: the nature of cyberspace as a 'complex adaptive' system and the ease of proliferation of cyber capabilities among offensive actors. This section will show that these characteristics are sources of uncertainty because they create an unpredictable environment populated by a diverse set of actors and agendas. The following section will elaborate on how complex adaptiveness and the ease of proliferation have implications for responses by increasing the risk of misattribution and the risk of unintended effects, including escalation.

Operational characteristic 1: Cyberspace as a 'complex adaptive' system

As operational environments go, cyberspace is a highly complex system, which can evolve in unpredictable ways [16, 61]. The US Army visualizes cyberspace as comprising three layers: the physical, logical and social layers, which in turn have five components: geographic space, physical network, logical network, persona and cyber persona [62]. The physical layer includes the physical location of the network's parts as well as all its hardware and infrastructure; the logical layer, software and lines of code that form connections between the hardware; and the social layer, the people actually on the

[12] Scholarly definitions of deterrence by denial broadly cluster around the notion of the 'threat that effective defences will defeat an attack' or a promise to prevent the opponent from achieving their objectives [21, 58].

[13] Some scholars would dispute this. Michael Fischerkeller, for example, argued that US policymakers have often viewed increasing resilience incorrectly as part of a strategy of deterrence by denial. According to Fischerkeller, deterrence by denial threatens the aggressor with a war of attrition, making aggression unprofitable—it has little to do with hardening the defence surface and more to do with capabilities. He concluded that increasing resilience can instead be better understood as being part of a *defence* strategy, that is, diminishing an adversary's ability to inflict damage, rather than a *denial* strategy, which, according to Fischerkeller, is structurally impossible in cyberspace [59].

network and their cyber personas (such as an IP address or email address), which can be multiple [62, 63]. In addition to the Internet of networked computers, there are also intranets, cellular technologies, fibre optic cables and space-based communications [61]. Complicating things further, as this intricate web of interconnections expanded during the Internet's development, network designers prioritized the convenience of connectivity over the necessity for security against computer-born threats [63, 64].

Charles Perrow, in his seminal work on 'normal accidents', pointed out that complex systems have the following characteristics: unfamiliar or unintended feedback loops, many control parameters with potential interactions, indirect or inferential information sources and operators' limited understanding of certain processes [15]. In a complex system, small differences in initial conditions can produce large changes in patterns of behaviour and unexpected strategic outcomes [66]. The interaction of these processes also has an enormous impact on the potential for system accidents and failure [15, 16]. While especially acute in the cyber context, the problem of complexity is not exclusive to it. Indeed, Perrow famously argued that normal accidents are inevitable in any complex system due to 'the way failures interact and the way the system is tied together' [15].

Other scholars have gone further: they have characterized the cyber domain as a complex *adaptive* system [65]. That is, in addition to the above characteristics, the system generates new knowledge that has causal properties of its own, which result in the adaptive behaviour of the system itself. As a result, the system evolves in ways that the system's designers themselves did not envisage [66]. Complex adaptive systems therefore tend to exhibit 'chaotic behaviour' [65], which complicates enormously the task of predicting their failure rates [63].

Then, there is the issue of interconnections among critical infrastructures. Much like a central nervous system, cyberspace runs through these infrastructures, including communications, emergency services, government, food, water, health, transport, finance and energy, allowing them to communicate and function [63]. By implication, a failure in one infrastructure has the potential to cascade into others, significantly raising the probability of unanticipated consequences [67]. More specifically, the vast majority of critical infrastructure is dependent on two particular interconnected physical and cyber-based control systems: supervisory control and data acquisition (SCADA) and distributed control systems (DCS) [62]. The near-ubiquitous employment of these systems results from the clear benefits they bring to operational efficiency: they allow the remote operation and maintenance of critical infrastructures in real time [68]. These systems, however, are inherently vulnerable as their communication is carried out through a variety of media, including Ethernet, wireless, shared leased lines and the Internet [69]. In addition, SCADA and DCS are also now built using commercial of-the-shelf components, some of which have known security vulnerabilities [69]. The European Union Agency for Network and Information Security has identified a number of plausible attack scenarios involving the exploitation of these vulnerabilities. One scenario envisages an attacker compromising the systems by taking control of one or multiple assets in the network and thereby manipulating them all—an intrusion that could potentially cause blackouts or service cuts if it involves the energy grid. Another scenario concerns malware infections during SCADA system maintenance and upgrade processes [68]. If the state of one critical infrastructure depends on information transmitted through another critical infrastructure, then an attack on one SCADA system can potentially produce a cascading failure [70].

The recently developed understanding within US Cyber Command of cyberspace as an environment of 'constant contact and shifting terrain,' which is 'continually at risk,' can be seen as a manifestation of the concern about the complexity and interconnectedness of the cyber operational environment [71]. We will return to the evolution of strategic thinking on cyberspace in the United States in the final section.

Operational characteristic 2: Ease of proliferation

A second operational characteristic that can become a source of uncertainty is the ease of proliferation of offensive cyber capabilities. The concept of proliferation means the acquisition of a pre-existing or similar capability by an actor other than its creator [72]. Generally speaking, there is a higher likelihood of proliferation and diffusion of cyber capabilities in comparison to kinetic weapons. Cyber capabilities, unlike kinetic weapons, do not necessarily destroy themselves upon use, meaning that their components may be repurposed [73]. And once a cyber capability has been developed, it can often be reverse engineered, making it far cheaper and easier to manufacture other capabilities [72]. With the right malware analysis expertise, an adversary is able to draw inspiration from or reuse the techniques, tools and procedures used in the different stages of a previous attack.[14]

To take an example, the EternalBlue exploit was likely first developed by the NSA and subsequently leaked online by a hacker group called the Shadow Brokers. EternalBlue exploits the CVE-2017-0144 vulnerability in the Server Message Block protocol, which is used in Windows machines to request files and print services from server systems over a network [75]. EternalBlue is therefore most useful for using remote services to move laterally within a network, thus enabling the fast spread of malware between systems [76]. Indeed, EternalBlue has been repurposed multiple times by groups other than the developer for the execution of widespread and damaging cyberattacks—most infamously in the cases of the WannaCry ransomware attack and NotPetya [77, 78].

In cases where the simple redeployment of an exploit or other technique is not possible—usually when a capability has been precisely designed to hit only one specific target—design emulation still remains an option for an aspiring proliferant [72]. This works by copying not lines of code, but the operation's design features (e.g., the method of entry). The case that most notably comes to mind is Stuxnet. While the worm that targeted the programmable logic controllers at the Natanz nuclear facility was highly customized and thus released its payload only within systems in the target facility, the attack tactics and technology were generic enough to be used against other targets [79]. Specifically, Stuxnet could serve as inspiration for designers of cyberattacks to exploit *physical* vulnerabilities in plant and control systems [79]. Exploiting flaws in the products and architecture of industrial control systems can be particularly attractive to an attacker because these vulnerabilities—unlike software vulnerabilities—cannot be patched and are therefore likely to remain exploitable for years [79]. Indeed, leaked NSA documents reveal that the Agency fears Iran will draw inspiration and operational ideas from western cyberattacks that targeted its infrastructure, including Stuxnet, Flame and Duqu, to develop its own similarly sophisticated operations [80].

[14] Attack stages include initial access, execution, persistence, privilege escalation, defence evasion, credential access, discovery, lateral movement, data collection, command and control, exfiltration and final impact [74].

The ease of proliferation has the effect of lowering the barriers to entry into the cyber domain for malicious actors. The multiplicity of offensive actors, from state agencies to hacker groups, has been studied extensively by scholars [21, 81–83]. Previously weak actors, including non-state actors, no longer need to develop weapons from scratch; they are able to quickly take advantage of the time it takes to patch systems and redeploy previously used capabilities or simply purchase them on illegal marketplaces. The range of scenarios and threats that might arise from rampant proliferation is difficult to predict. The gains of intelligence agencies and cyber units that stockpile exploits can quickly be translated into losses if capabilities are stolen or 'escape' in testing stages.

Concerns about capability proliferation have often been highlighted by US government officials. 'In a future conflict', wrote Obama in an op-ed, 'an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities at home' [84]. Obama's Secretary of Defense, Chuck Hagel, voiced similar concerns: 'Our nation confronts the proliferation of destructive malware and a new reality of steady, ongoing and aggressive efforts to probe, access, or disrupt public and private networks and the industrial control systems that manage our water and our energy and food supplies'.[15] In a speech in October 2020, Christopher Ford, President Donald Trump's Assistant Secretary for International Security and Nonproliferation, referring specifically to concerns about risk, highlighted that, 'effective risk reduction in the cyber domain is challenged by several important characteristics of the cyber domain', including the difficulty of attribution, the 'ubiquity and often dual use nature' of cyber capabilities and their 'possession by both state and non-state actors'.[16] Thus, the combination of the domain's empowerment of militarily weaker actors and America's own digital dependence means that US policymakers have often felt that their country is asymmetrically vulnerable in cyberspace.[17]

Cyberspace and uncertainty: How operational characteristics complicate responses to cyberattacks

Having reviewed the operational characteristics of cyberspace that are most problematic for the United States as a risk society, let us now explore how they pose an obstacle to the application of meaningful responses.

The risk of misattribution

The structural complexity of the cyber domain and the wide universe of possible perpetrators as a result of proliferation, coupled with availability of anonymity-enhancing tools and techniques, lengthen the forensic process of attributing attacks [87]. While scholars have shown that technical attribution of a cyber incident is usually possible, the analysis of an operation within a narrow timeframe is nevertheless challenging even for well-resourced teams [81].

The difficulty of attribution is a particular problem for risk societies. As we discussed, risk societies abhor uncertainty; they will generally not issue a meaningful response while there is even the slightest risk of misattribution as this could lead to unintended and unpredictable consequences, including triggering an unwanted conflict or diplomatic standoff. In addition, risk societies, as societies frightened particularly by unpredictability, are more likely to want to engage in public attribution in order to establish international rules of behaviour to 'stabilize a particular interaction order' [88]. The process of public attribution, which falls under the rubric of what Florian Egloff terms the 'meaning-making process', defined as the national security process concerned with the communication of the attribution judgement to others in order to exert political effects, can take even longer than technical attribution [88]. Concerns about not revealing sensitive sources and methods that informed an intelligence assessment, the reliance on which is often a necessity due to the aforementioned tools and features that that help obfuscate an attack perpetrator's identity, are an important complicating factor in this regard [88]. Thus, the length of time that it takes risk societies to confidently and publicly attribute an operation to a single state actor often means that they are not able to conclude the attribution process in the time they have to respond meaningfully (recall that swiftness is a key element of a meaningful response).

The complexity of attribution is illustrated by recent cases. WannaCry and NotPetya demonstrated that an attack's level of sophistication is not necessarily the most reliable indicator of the perpetrator; this observation goes against analyses that argue that the most damaging attacks can be more easily attributed because few actors are in possession of the type of capabilities needed to execute and benefit from them [21]. In the case of WannaCry, neither the ransomware nor the delivery methods were sophisticated. In fact, cybersecurity researchers, having found numerous bugs in the code, initially speculated that the malware had 'escaped' from its authors in the development stages [89]. The element of WannaCry that was more advanced was the EternalBlue exploit, but, as we discussed, this NSA-developed exploit was simply repurposed after having been leaked online [90].

In both the WannaCry and NotPetya cases, the length of time that it took victim states to issue public attribution statements is evidence in itself of the complexity of the process, both from a technical and a political standpoint. The attacks took place in May 2017 and June 2017, respectively, but formal attribution statements were issued months later in December 2017 and February 2018, also, respectively [23, 34].

The case of NotPetya further illustrates how a lengthy process of attribution, characteristic of risk societies, interfered with the imposition of meaningful penalties. The enormous delay in publicly attributing the operation meant that other events came to pass in the interim, resulting in the punishment of NotPetya no longer being a high priority on policymakers' agendas or at the forefront of public attention. The day after the White House publicly attributed the operation to Russia on 15 February 2018, the US Justice Department issued a momentous indictment of 13 Russian officials and three companies, including the now infamous Internet Research Agency, for interfering in the 2016 presidential election [91]. The indictment and the revelation of a sweeping Russian disinformation campaign dominated headlines and consumed the attention of the public as well as policymakers [92]. Thus, when the Treasury announced a sanctions package in March 2018, it became apparent that the sanctions did not punish NotPetya specifically, but instead were a response to a whole host of different Russian cyber activity, 'ranging from interference in the 2016 US elections to conducting destructive cyber-attacks, including the NotPetya attack' [93]. In addition to sanctioning the Russian Federal Security Service and Main Intelligence Directorate as well as and six individuals for broad cyber-enabled activity, which included NotPetya, the Treasury

[15] Hagel quoted in [85].

[16] Ford quoted in [86].

[17] Author's personal interview with Michael Daniel, 10 September 2020.

sanctioned a different set of entities and individuals, those that had been listed in Special Counsel Mueller's indictment (including the Internet Research Agency), for a different set of effects, namely election interference [93].

The connection between the act and the response was therefore heavily muddied by events that had come to pass in the interim. And although the US Treasury referred to NotPetya in announcing the sanctions, the long list of Russian misdemeanours included in the same press release significantly diluted its meaning. What's more, the intent behind NotPetya to this day remains ambiguous, while the intent behind the election campaign was clearly stated in the indictment as being the undermining of trust in the US political system [94]. An attempt to punish general 'malign Russian cyber activity' in one action, and the lack of differentiation between the attacks, seemed to signal to Russia that it was being punished on the basis of the *means* employed in the attacks, rather than for the *intent* behind the operations or their *effects*. Having not differentiated between operations, the response to Russia's cyber activities, including NotPetya, was therefore unlikely to have given the enemy, in Schelling's words, 'a basis for judging what to expect as the consequences of his own actions', which Schelling explains is a crucial element of meaningful punishment [95].

NotPetya was once again mentioned among a list of operations, including attacks that attempted to 'undermine, retaliate against, or otherwise destabilize' Ukraine, Georgia, the French presidential elections, investigations into the Russian Novichok attack and the 2018 PyeongChang Winter Olympic Games, in a much later indictment in 2020 of six Russian GRU (military intelligence) officers [96]. The decision to list a number of cyber operations with enormously differing effects, from spear-phishing for the purposes of espionage to the disruption of electricity supplies in Ukraine [96], meant that it suffered from the same signalling problems as the 2018 sanctions package and sent a confusing message to the Russians regarding so-called red lines.

From a risk avoidance perspective, it is not surprising that the United States often chooses indictments over other forms of response. Criminal charges require a higher burden of proof than standards of information that typically form the basis for national security decision-making; prosecutors must be prepared to prove 'beyond a reasonable doubt' that a party is guilty before an independent judge and jury [97]. Striving to avoid uncertainty in attribution, in the midst of knowledge of the difficulties of this due to the nature of the operational environment, issuing indictments is a procedural way of addressing the potential risks that would result from misattribution. Indictments communicate a high level of confidence in the attribution judgement to the adversary, thus decreasing the risk that the adversary will be able to credibly rebuff the statement. Finally, they also satisfy the need to demonstrate to domestic publics that 'something is being done', while avoiding the risks that stronger response might entail.

The risk of unintended effects: Collateral damage, blowback and escalation

Other considerations arising from operational uncertainty that mar the response calculus in risk societies are first, the unintended effects of the initial attack, which can interfere with the victim's interpretation of the attack's intent and make it difficult to determine a timely and appropriate response, and secondly, an awareness that a potential response might also entail unintended effects such as collateral damage, blowback or escalation.

In kinetic military operations, collateral damage refers to physical damage to a civilian target or civilian deaths resulting from an offensive action [98]. The concept is key to the discussion of proportionality in the Geneva Conventions. There exists a well-defined methodology for assessing and anticipating collateral damage from conventional military actions [98, 99]. The same is not true for cyber actions, which is problematic for cyber responses because there is a greater potential for collateral effects in cyberspace than in physical space [98]. In fact, the high degree of interconnectedness between systems and between the external functions they support (operational characteristic 1) means that a cyberattack can cause indirect effects that surpass the direct effects on the target systems themselves. Cascading collateral damage can therefore impact vital activities across a wide range of interests and complicate both the interpretation of the initial attack and the design of an appropriate response [72]. While scholars have argued that cyber weapons are not inherently indiscriminate [73], the unplanned spread of malware remains a concern among risk-conscious decision-makers. In his memoirs, Clapper wrote that 'reciprocity and collateral damage in cyberspace are very difficult to control. . . . So if we attacked someone in cyberspace and they returned fire . . . the New York Stock Exchange or telecommunications in Eastern Europe or a power grid in Central America might well be taken offline. No one could predict the unintended consequences and potential damage such an assault could cause' [27].

A second problem arising from the high probability of unintended effects of operations in the cyber domain is that a cyberattack in response to an adversary, cyber retaliation, can be counterproductive if its spread or collateral damage is so substantial that it generates blowback. As we mentioned earlier, this is especially troubling because Schelling advises that ideally, a meaningful response should be mounted in the same 'currency' [95].

Blowback from a cyber response can happen in two ways. First, malware used in a retaliatory attack can inadvertently spread between machines and damage the retaliator's own infrastructure or that of allies. This tends to occur in the case of poorly customised capabilities, such as those targeting near-ubiquitous Windows operating systems [72]. An illustrative example of a cyberattack (not retaliatory in this case) having unintended effects is again the NotPetya attack, which, like WannaCry, took advantage of the Windows EternalBlue exploit discussed earlier. While the attack was traced back to the Russian state, it was found to have affected large Russian companies, such as Rosneft, as well [22]. A second form of blowback occurs when a cyberattack targeting a single institution ends up disrupting assets in a public commons, such as nodes in the global financial system, due to the interconnectedness of computer systems [72]. Such a situation has not yet fully materialized, but hints at its occurrence exist. NotPetya, for instance, had a significant impact on global shipping and trade. Although the attack was meant to target systems in Ukraine, it brought Maersk, a company that carries one-fifth of the world's entire shipping cargo, to a standstill for a period of two weeks [22]. NotPetya therefore represents a combination of two types of blowback.

Conscious of the potential for blowback, victims might be more cautious in responding to a cyberattack using the same means for fear of their retaliatory operation or the aggressor's response to the retaliation affecting their own (or allies') digital infrastructures. This is especially the case if a state like the United States is more vulnerable to cyberattacks than its adversaries, having prioritized innovation and connectivity at the expense of systems security [18]. Savvy aggressors may even be aware of the fact that presently, cyberattacks are unlikely to be included in a retaliatory package from a risk-averse country like the United States due to its sensitivity to unintended consequences [100].

The risks of blowback and unintended consequences restrain risk-averse nations in the application of economic sanctions too. Indeed, the United States has previously backed down from applying sanctions that might end up having adverse consequences for its domestic economy; an example was the 2019 removal of Rusal from the US sanctions list due to the concerns of US corporations about a steep rise in global aluminium prices resulting from the measures imposed on Rusal [101]. The concern about blowback from sanctions has also restrained their application in response to cyberattacks. In a personal interview on the subject, Michael Daniel, former Cybersecurity Coordinator on the National Security Council, explained that states must be 'very judicious' about how they use financial sanctions as a tool of response to hostile cyber operations because of the possibility that eventually the targeted states might embark on setting up an alternative financial system and 'completely bypass New York'.[18]

A third possible unintended effect resulting particularly from cyber retaliation is escalation. Inadvertent or accidental escalation can occur when one party's actions are interpreted as escalatory by the other party to a conflict, and this party issues a stronger counter-response [102]. As Ben Buchanan wrote, the dilemmas of interpretation of intent are particularly pronounced in cyberspace [103]. Accidental escalation can happen as a result of signalling issues, which are born from the fact that cyberspace is constantly full of activity (recall operational characteristic 2—proliferation and the diversity of actors), making it difficult for a state to recognize clear signals of what an adversary wants to achieve through a cyberattack [102]. Additionally, as we discussed, problems of interpretation of attacks may result from excessive damage to unintended targets; it is not easy to quickly design cyber operations that are fully predictable and carefully calibrated in terms of their force [73, 102, 104]. The next section will explain how escalation concerns bred restraint in the American responses to the 2013 distributed denial of service (DDoS) attacks and the 2016 election interference.

Altogether, the characteristics of the cyber domain—including the system's emergent complexity and the ease of proliferation and the consequences of these in terms of breeding uncertainty in attribution and uncertainty of the effects of a cyber response—are likely to lead risk-conscious policymakers towards restraint in the design of individual responses, or even the decision not to respond at all. Additionally, the perception of cyberspace first and foremost as a domain of uncertainty means that risk societies will approach it differently than states with a higher risk threshold. They are more likely to employ strategies that minimize as much as possible, first, the occurrence of cyberattacks through preventive action and improving defences and, secondly, if that fails, seek to manage their harmful consequences. They do this using risk management, which, as we have discussed, includes preventive action, increasing resilience and consequence management. In the following section, we turn to exploring how these practices have been applied as part of the US approach to the cyber domain.

US Risk management: Moving from caution to proactiveness

This section conducts an empirical case study to illustrate the risk society arguments of previous sections. The discussion will first focus on the Obama administration and show how concerns about unintended effects, particularly regarding escalation, led to the abandonment of meaningful punishments for cyberattacks. It will then explain how the administration put in place the practices of increasing resiliency and consequence management and began to consider preventive action. The next part will consider the Trump administration, showing how the understanding of the cyber operational environment evolved to produce new ideas on how to engage in inter-state competition in this domain.

Obama administration

During Obama's presidency, deterrence through and from cyberspace was in vogue. The administration's stated willingness to dissuade the adversary from conducting cyberattacks, both through denial and punishment, was set out in a number of official documents [105]. For example, a White House Report on Cyber Deterrence Policy envisaged creating 'strong defences and architect[-ing] resilient systems that recover quickly from attacks or other disruptions' combined with 'measures [that] are designed to both threaten and carry out actions to inflict penalties and costs against adversaries that choose to conduct cyber attacks' [2]. A Department of Defense (DoD) Cyberspace Policy report to Congress explained that, 'should the "deny objectives" element of deterrence not prove adequate, DoD maintains, and is further developing, the ability to respond militarily in cyberspace and other domains' [106]. The 2011 International Strategy for Cyberspace promised that 'certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners' [105].

Yet, as we discussed already, state practice diverged from official policy. Rather than employing deterrence, the way in which the Obama administration actually reasoned about responding to attacks in the cyber domain was primarily through the lens of risk. Two instances where the United States was faced with the dilemma of how to respond to a cyberattack demonstrate risk thinking in terms of clear concerns about America's asymmetric vulnerability and the risk of unintended effects, particularly escalation. The first occurred between December 2011 and May 2013 when the US financial sector was plagued by a long campaign of Iranian DDoS attacks, known as Operation Ababil [107]. According to James Clapper, a retaliatory strike had been considered. 'The initial instinct was: Let's attack back' [108]. Ultimately, however, even a relatively mild action like breaching servers on Iranian networks to halt the attacks at their source raised concerns about escalation, particularly in the form of a counterattack on US banks [108, 109]. Clapper explained: '. . . if you attack them, you have to anticipate a probably much . . . greater retaliation as a result' [108]. A former senior NSA official added that Iran was more likely to see itself as an 'insurgent' rather than a 'stakeholder' in the stability of the international monetary system and therefore would have less to lose in launching a counterattack (i.e. Iran was seen as being comparatively less vulnerable to blowback from a cyber strike of its own) [108]. Unintended effects, and the perceived high probability of Iran launching a damaging counter-response, thus ultimately led to a rejection of meaningful punishment.

Concerns about unintended effects were also paramount when the White House was in the process of deciding on how to respond to Russian election interference in 2016. Importantly, American officials had considered strong punishments in line with the warnings that had been issued to Russia in September and October of

[18] Author's personal interview with Michael Daniel, 10 September 2020.

that year [110, 111]. Investigative reporting revealed that after learning about the Russian intelligence service's campaign to disrupt the elections, Obama approved a covert measure authorising the planting of damaging cyber capabilities in Russian infrastructure [110]. The administration had also contemplated the release of compromising material and sanctions that could 'crater' the Russian economy [110]. A detailed report shows that the reason they did not implement these was a recurring concern that 'any pre-election response could provoke an escalation from Putin', potentially in the form of a cyber operation targeting voting systems [110]. The attention that decision-makers paid to potential unintended effects as a result of a response is corroborated by three further accounts.[19] One anonymous principal decision-maker explained that, 'If we got into a tit-for-tat on cyber with the Russians, it would not be to our advantage. ... They could do more damage to us in a cyber war or have a greater impact' [111]. Clapper was concerned about a potential Russian counter-response targeting American critical infrastructure, particularly electrical grids [111]. Benjamin Rhodes, Obama's Deputy National Security Advisor, wrote that Obama himself was worried about Russia hacking into Election Day vote tabulations [113]. Concerns about cyber escalation ultimately resulted in the decision of policymakers to abandon meaningful reprisal.

During the Obama administration, policymakers' view of the operational environment was also consistent with that of a risk society, a society that Christopher Coker described as being 'permanently on the defensive' [19]. In a 2016 interview for *Wired Magazine*, Obama himself emphasized the need to 'think differently about our security' and take a public health model in dealing with problems in the cyber domain, which are more akin to viruses and pandemics than 'a bunch of tanks rolling at you'.[20] In an effort to implement this thinking, the Obama administration focused mainly on the risk management practices of increasing resilience and consequence management. Later, it also started to move towards preventive action with the introduction of 'active defence'.

Bolstering resiliency as a practice was most visible in the administration's efforts to improve cyber hygiene practices and increase information sharing between the private and public sector. A 2013 executive order bound US government entities to disclose detected breaches to private sector companies [115]. Then, the Cybersecurity Information Sharing Act was signed into law in late 2015, encouraging companies to share information and authorising them to implement defensive measures on their systems to counter cyber threats [116]. Another example of a resiliency initiative was the Cybersecurity Sprint, introduced by the White House in June 2015. The objective was to improve computer hygiene across the US government in 30 days, by introducing ubiquitous multifactor authentication, limiting the number of users with administrative privileges and installing software patches [117].

The Obama administration also demonstrated a preference for consequence management. This was particularly visible in the reaction to the aforementioned Iranian DDoS attacks on the US financial sector. US State Department and Homeland Security officials solicited the help of 120 countries to disrupt botnets on their territories that, unbeknownst to these countries, were routing the attacks. Allies' computer emergency response teams were instructed to employ blackhole filtering, a process by which undesirable network traffic is forwarded and dropped at the edge of a network [109, 118]. They were also asked to patch vulnerabilities in their systems to lock the adversary out. Importantly, the whole operation was conducted without encroaching on Iranian networks [109].

Preventive risk management in cyberspace, albeit under the rubric of 'pre-emption', was encouraged as early as 2010 by Mike McConnell who had been the director of the NSA under President Bill Clinton. McConnell stated that pre-emption in cyberspace should be akin to US efforts in counterterrorism and involve 'degrading, interdicting and eliminating ... [adversaries'] leadership and capabilities to mount cyber attacks' [119]. Eventually, flavours of this approach could be found in the strategy of active defence.

Active defence as a concept goes back as far as 1996. Although its definition has been through multiple iterations, it is generally understood to mean the US DoD engaging in defensive activities outside its own networks [120]. The crucial element of active defence refers to the proactive anticipation and disruption of future attacks before these hit US territory [83, 121]. In practice, this meant using 'sensors, software, and intelligence to detect and stop malicious activity before it [could] affect DoD networks and systems' [122]. In the event that malware did pass through undetected, it also foresaw hunting for the adversary within the DoD's own networks [121]. As we will discuss next, elements of the Obama administration's active defence seemed to be a pre-cursor to the later strategies of persistent engagement and defend forward introduced under the Trump administration in 2018.

Trump administration

The resiliency efforts initiated by the Obama administration were taken further by the Trump administration with the creation of the Cybersecurity and Infrastructure Security Agency, which has a specific mandate to increase the resilience of US critical infrastructure [123]. Increasing resiliency for the purposes of 'reducing the size of the attack surface at home' also appeared as a stated goal in the 2018 Command Vision for US Cyber Command (CYBERCOM) [71]. The recent activities of US Cyber Command in terms of publicly disclosing malware tools on Virus Total, an online repository, are another textbook example of increasing resilience. In a notable disclosure, Cyber Command specified that the malware samples it had uploaded had been attributed to North Korea and had aided the regime in pursuing illegal activities, including the stealing of funds for sanctions evasion [124]. The purpose of publicly disclosing the tools is to enable the private sector to build better defences, thus decreasing the impact of future cyberattacks and helping safeguard the health of the American economy [125].

A more distinctive risk management practice under the Trump administration was preventive action. Spearheaded by US CYBERCOM, there was a substantial change in 2018 in American cybersecurity thinking [126–128]. The strategies of persistent engagement and defend forward are grounded in an understanding of cyberspace as an environment of 'constant contact' and 'shifting terrain' [71]. The CYBERCOM Command Vision document explains that, by continually burrowing deep into US networks, adversaries force the USA into a 'reactive mode', which 'introduces unacceptable risk to our systems, data, decision-making processes, and ultimately our mission success' [71]. General Paul Nakasone, Commander of CYBERCOM and Director of NSA, clarified in an interview that threats in cyberspace 'persist because the barriers to entry are low and the capabilities are rapidly available and can be easily repurposed' [129]—referring pointedly to operational characteristic 2 discussed earlier. Adapting to this new strategic

[19] These accounts were first discussed by Bruce Schneier in a blog post [112].

[20] Obama quoted in: [114].

environment, CYBERCOM shifted from being a 'response force' to a 'persistence force' [130]. There is a clear preventive focus in its new strategy: 'We should not wait until an adversary is in our networks or on our systems to act with unified responses across agencies regardless of sector or geography' [71]. General Nakasone believes that US adversaries have long been engaging in cyber operations 'to gain advantage without escalating to armed conflict' [131]. Even without crossing into armed conflict, however, adversarial operations are still seen as unacceptable to the United States because they degrade sources of national power [132]. Rather than issuing punishments for these operations, however, the United States as a risk society chooses instead to prioritize preventive action.

One of the major concerns about the new US approach has been the idea that a more forward-leaning US posture might produce unintended conflict escalation [120]. This is because the strategy of persistent engagement introduces greater levels of uncertainty and friction for the adversary, which is known to intensify conflicts; competitive activity may also be subject to misinterpretation as offensive action, given the limitations of effective signalling in cyberspace as we discussed earlier [133]. These concerns are compounded by the fact that the Command Vision document seemingly omits a discussion of how to mitigate escalation [133].

It may therefore seem somewhat paradoxical that the new preventive strategies are actually an outgrowth of the US risk society's overarching objective of managing future risks and uncertainty and, within this, escalation. Persistent engagement campaigns are intended to be limited and measured by design, precisely to prevent triggering a response from adversaries that could escalate into a wider conflict [134]. General Nakasone, Commander of CYBERCOM and Michael Sulmeyer, Nakasone's Senior Adviser, wrote that reducing the risk of escalation was a 'critical part of the planning process' for a more proactive US stance in cyberspace and pointed out that 'inaction poses its own risks' in terms of allowing damaging cyber campaigns to continue to penetrate US systems [135].

Furthermore, most actions under persistent engagement are understood to be covert in nature. Indeed, Lennart Maschmeyer argues that in order to be successful, they must be both covert and clandestine, as otherwise they risk being prematurely neutralized [136]. Hiding such operations from outside audiences, while potentially problematic for reasons of public accountability, can in itself be an indication of restraint and wanting to manage the risk of escalation by keeping the rivalry 'under the radar'.[21]

Because of their covert nature, we have only had rare glimpses into the operations of Cyber Command since the strategy came into place. In February 2019, we learned about how American operatives took down the servers of the Russian Internet Research Agency in an effort to prevent the kind of interference in the mid-term elections that the Agency had orchestrated during the 2016 presidential vote [138]. But even this operation came to light months after its execution and the details were superficial: one US senator, having listened to a classified briefing on the operation, lamented the fact that the American public would not be able to learn more about its achievements [139]. What we do know is that the operation was non-violent and did not appear to provoke a public reaction or retaliation from Russia.

As we discussed earlier, prevention as a risk management strategy was first implemented as part of President George W. Bush's 2002 National Security Strategy and was widely criticized on the grounds of embroiling the United States in protracted wars in the Middle East. Undoubtedly, the geopolitical and operational context within which persistent engagement has been introduced is very different. There are, however, notable overlaps in the guiding assumptions of the two strategies. In both cases, there is a marked emphasis on urgency of action and the necessity of disrupting potential threats before they materialize. For example, the 2002 Strategy stressed the need to abandon a reactive posture due to the 'immediacy of today's threats' [140]. The overall focus of the Strategy was prevention (which had mistakenly been called pre-emption [86]) and 'anticipatory action' [140]. Similarly, the 2018 DoD Cyber Strategy stresses the need to 'pre-empt' hostile cyber actions and 'defend forward by leveraging our focus outward to stop threats before they reach their targets' [141]. The Cyber Command Vision cautions that a 'reactive posture introduces unacceptable risk' [71].

The major important change is the inherently uncertain operational environment in which states now compete with each other: cyberspace. In analysing US responses to cyberattacks and the evolution of the country's cyber policy, we see an adaptation of risk management strategies used for counterterrorism during the Bush era to this new environment. The key difference is the definitive move away from violence and overt aggression towards non-violence, covertness and continuous engagement in preventive practices. Whereas under Bush prevention meant armed intervention, in the context of the cyber domain under the Trump administration it meant encroaching on enemy territory, red space, to disrupt adversary operations and capabilities covertly and without the use of force. In communicating more openly about persistent engagement and defending forward, the United States has sought to signal to adversaries its non-escalatory intent and thereby limit misperception. By establishing a constant presence in adversary networks, it is possibly trying to gain a solid understanding of these systems, which should help to minimize the unintended effects of any subsequent operations in those networks. The result of preventive practices is therefore unlikely to be escalation into wider conflict, making them the ideal choice for risk-intolerant societies. Instead of escalation, what we are more likely to see over time is a normalization of preventive risk management practices in a largely invisible realm where public accountability and audience costs are low and therefore regulation and oversight are near impossible.

Conclusion

In posing the question of why the United States does not respond meaningfully to cyberattacks, this article has presented four main arguments. First, it claimed that US policymakers are guided in their approach to the uncertainty of cyberspace by the dominant 'risk management' paradigm, which includes addressing cyber-related challenges through the practices of preventive action, increasing resilience and consequence management. Second, it explained the characteristics of cyberspace that make it a highly uncertain operational environment. Third, it showed how these characteristics lie at the root of risk societies' response dilemma in terms of increasing

[21] The desire for escalation avoidance is also evident in recent academic scholarship, particularly in the work of Richard Harknett, Emily Goldman and Michael Fischerkeller, all of whom have been influential in informing the new strategies [39, 133]. Addressing the issue of escalation specifically, Fischerkeller and Harknett have sought to show that persistent engagement will 'inhibi[t] adversary efforts to increase the scale, scope and/or intensity of cyber operations/campaigns' and therefore maintain competitive interaction dynamics below the threshold of armed conflict and within the bounds of agreed competition [133].

the risk of misattribution and the risk of unintended effects, including collateral damage, blowback and escalation. Fourth, the article demonstrated that all three risk management practices are visible in US policy and practice in cyberspace from the Obama administration through to the Trump administration. Although the paper presented a single case study from which it is difficult to generalize, scholars might want to apply the risk framework to other contexts, including for example the UK.

The paper suggested that the practice of preventive action, which has evolved significantly since its last ill-fated appearance in US policy under Bush, has become the risk society's answer to dealing with operational uncertainty. While it is unlikely that preventive risk management will escalate into more intense conflict, we need to urgently examine what happens when a vast amount of great power competition is largely invisible to the public eye. What happens when preventive risk management is covert and clandestine? Will this situation, following Austin Carson's work on 'secret wars', provide opportunities for great power collusion on the 'cyber backstage' during times of geopolitical tension [137]? Or will it normalize the existence of a cyber 'wild west', devoid of regulation and oversight, where not only the United States but also its adversaries will have free rein in 'red space'? Beck had his own term for this potential scenario: 'the boomerang effect', whereby risk management practices ironically produce new and unforeseen risks of their own [11].

Acknowledgements

The author would like to thank the two anonymous reviewers, the editors of the Special Issue, Josh Goldstein and Lucas Kello for their insightful feedback, and Richard Harknett, Michael Fischerkeller and Max Smeets for their helpful comments on an early draft. The author is grateful to have had the opportunity to present the research of this paper at the 2019 Hague Cyber Norms Conference, the 2019 and 2018 Bridging the Gap Workshops, the 2019 Oxford University Changing Character of War Annual Conference and the 2018 Oxford University Centre for Doctoral Training Showcase.

Funding

The work of the author and the Hague Program for Cyber Norms is generously supported by a grant from the Dutch Ministry of Foreign Affairs.

Conflict of interest statement. The author declares no conflict of interest.

References

1. The White House. *National Cyber Strategy of the United States of America*. Washington, DC: The White House, 2018.
2. White House. Report on Cyber Deterrence Policy, 2015.
3. King A, Gallagher M (eds). *United States of America Cyberspace Solarium Commission*, solarium.gov 2020.
4. Department of Defense. *Department of DefenseDefense Science Board Task Force on Cyber Deterrence*. Washington, DC: Department of Defense, 2017.
5. Rid T. Deterrence beyond the State: The Israeli Experience. *Contemporary Security Policy* 2012;**33**:124–47.
6. Schelling TC. *Arms and Influence*. New Haven: Yale University Press, 2008.
7. Voo J, Hemani I, Jones S, *et al*. *National Cyber Power Index 2020*. Boston, MA: Harvard Kennedy School Belfer Center for Science and International Affairs, 2020, 84.
8. International Telecommunications Union. *Global Cybersecurity Index (GCI) 2018*. Geneva, Switzerland: International Telecommunications Union, 2019.
9. Cyber Power Index. *Economist Intelligence Unit and Booz Allen Hamilton*. McLean, Virginia: Booz Allen Hamilton, 2011.
10. Goldsmith J, Russell S. *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations*. lawfareblog.com, 2018.
11. Beck U. *Risk Society: Towards a New Modernity*. London: SAGE, 1992.
12. Giddens A. Risk Society: the Context of British Politics. In: Franklin J (ed.), *The Politics of Risk Society*. Cambridge: Polity Press, 1998.
13. Williams MJ. (In)Security studies, reflexive modernization and the risk society. *Cooperation and Conflict* 2008;**43**:57–79.
14. Heng Y-K. *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*. London, UK: Routledge, 2006.
15. Perrow C. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books, Inc., Publishers, 1984.
16. Stevens T. *Cyber Security and the Politics of Time*. Cambridge, UK: Cambridge University Press, 2016.
17. Kello L, Richard T. Les cyberarmes: Dilemmes et futurs possibles. *Politique Étrangère* 2014;**Hivr**:139–150.
18. Clarke RA, Knake RK. *Cyber War: The Next Threat to National Security and What to Do about It*. 1st ed. New York: Ecco, 2010.
19. Coker C. *War in an Age of Risk*. Cambridge: Polity Press, 2009.
20. National Security Agency. *Iran – Current Topics, Interaction with GCHQ*, theintercept.com 2013.
21. Lindsay JR. Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity* 2015;**1**: 53–67.
22. Greenberg A. The Untold Story of NotPetya, The Most Devastating Cyberattack in History. *Wired Magazine*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (22 August 2018, date last accessed).
23. White House. *Statement from the Press Secretary*, whitehouse.gov 2018
24. Cimpanu C. Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack. *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/ (25 January 2018, date last accessed).
25. Nakashima E. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. *The Washington Post*. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.921e483e9b94 (1 December 2018, date last accessed).
26. Ng A. US sanctions Russia for election interference, cyberattacks. *CNET*. https://www.cnet.com/news/russia-faces-us-sanctions-for-election-interference-cyberattacks/ (15 March 2018, date last accessed).
27. Clapper JR. *Facts and Fears: Hard Truths from a Life in Intelligence*. New York: Penguin Random House Large Print, 2018.
28. Isikoff M. Ex-sanctions czar bashes Obama administration's "weak" response to Russian interference. *Yahoo News*. https://www.yahoo.com/news/ex-sanctions-czar-bashes-obama-administrations-weak-response-russian-interference-122944195.html (16 September 2020, date last accessed).
29. Blake A. Analysis | 'I feel like we sort of choked': Obama's no-drama approach to Russian hacking isn't sitting well. *Washington Post*. https://www.washingtonpost.com/news/the-fix/wp/2017/06/23/the-russia-2016-blame-game-finds-obama/ (16 September 2020, date last accessed).
30. Senate Committee on Armed Services. *Advance Questions for Vice Admiral Michael* S. *Rogers*, USN Nominee for Commander, United States Cyber Command, 2014.
31. Blake A. Analysis | NSA director Mike Rogers's remarkable comments about Trump's Russia efforts – or lack thereof. *Washington Post*. https://www.washingtonpost.com/news/the-fix/wp/2018/02/27/nsa-director-mike-rogerss-careful-indictment-of-trumps-anti-russia-efforts/ (21 September 2020, date last accessed).
32. Smart W. *Lessons Learned Review of the WannaCry Ransomware Cyber Attack*. Department of Health and Social Care and NHS England, 2018.

33. Dearden L. NHS to spend £150m on cyber security to bolster defences after WannaCry attack. *The Independent*. https://www.independent.co.uk/news/health/cyber-attacks-nhs-wannacry-security-investment-microsoft-a8327091.html (28 April 2018, date last accessed).
34. Foreign and Commonwealth Office. Foreign Office Minister condemns North Korean actor for WannaCry attacks. gov.uk 2017.
35. Schneider JG. Deterrence in and through Cyberspace. In: Lindsay JR, Gartzke E (eds.), *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford: Oxford University Press, 2019.
36. Bodeau D, Graubart R. *Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment*. Bedford, MA: The MITRE Corporation, 2013, 51.
37. Hodgson Q, Ma L, Marcinek K. *Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace*. Santa Monica, CA: RAND Corporation, 2019.
38. Harknett RJ, Smeets M. Cyber campaigns and strategic outcomes. *Journal of Strategic Studies* 2020:1–34.
39. Goldman E. (2020) From reaction to action: Adopting a competitive posture in cyber diplomacy. *Texas National Security Review*.
40. Beck U, Giddens A, Lash S. *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*. Cambridge: Polity in Association with Blackwell, 1994.
41. Hameiri S, Kühn FP. Introduction: Risk, risk management and international relations. *International Relations* 2011;**25**:275–9.
42. Gompert DC, Libicki M. Waging Cyber War the American Way. *Survival* 2015;**57**:7–28.
43. Beck U. *World Risk Society*. Cambridge: Polity, 1999.
44. Rasmussen MV. *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*. Cambridge: Cambridge University Press, 2006.
45. Heng Y-K. The continuing resonance of the war as risk management perspective for understanding military interventions. *Contemporary Security Policy* 2018;**39**:544–58.
46. European Commission, Environment Directorate-General, University of the West of England B, *et al. The Precautionary Principle: Decision-Making under Uncertainty*. Brussels, Belgium: European Commission, 2017.
47. Garrett NG. NATO, Security and Risk Management: from Kosovo to Kandahar, by Williams, M. J. *The Journal of Slavic Military Studies* 2010;**23**:525–7.
48. Coker C. Between Iraq and a hard place. *The RUSI Journal* 2006;**151**: 14–19.
49. Williams MJ. *NATO, Security and Risk Management: From Kosovo to Kandahar*. London, New York: Routledge, 2010.
50. Dupont B. The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity* 2019;**5**: 1–17.
51. Blanchard BW. Guide to Emergency Management and Related Terms, Definitions, Concepts, Acronyms, Organizations, Programs, Guidance, Executive Orders & Legislation: A Tutorial on Emergency Management, Broadly Defined, Past and Present, 2008.
52. Kreps S, Schneider J. Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. *J Cyber Secur* 2019;**5**:1–11.
53. Nichols TM. *Eve of Destruction [Electronic Resource]: The Coming Age of Preventive War*. Philadelphia: University of Pennsylvania Press, 2008.
54. Gray CS. *National Security Dilemmas [Electronic Resource]: Challenges and Opportunities*. 1st ed. Washington, DC: Potomac Books, 2009.
55. Doyle MW. Striking First. In: Macedo S (ed.) Striking first: preemption and prevention in International Conflict, Princeton, NJ: Princeton University Press, 2008.
56. Betts RK. Striking first: A history of thankfully lost opportunities. *Ethics & International Affairs* 2003;**17**:17–24.
57. Nye JS. Deterrence and dissuasion in cyberspace. *International Security* 2017;**41**:44–71.
58. Wirtz JJ. How does nuclear deterrence differ from conventional deterrence? *Strategic Studies Quarterly* 2018;**12**:58–75.
59. Fischerkeller MP. *The Structural and Strategic Imperative: The Need for Persistent Engagement*. Washington, DC: IDA Institute for Defense Analyses, 2018.
60. European Commission. *Annual Work Programme 2010: Prevention, Preparednesss and Consequence Management of Terrorism and Other Security Related Risks*. European Commission. ec.europa.eu 2010.
61. Nye JS. From bombs to bytes: Can our nuclear history inform our cyber future? *Bulletin of the Atomic Scientists* 2013;**69**:8–14.
62. United States Army. Cyberspace Operations Concept Capability Plan 2016-2028. 2010.
63. Clemente D. *Cyber Security and Global Interdependence What is Critical?* London: Chatham House, 2013.
64. Clark D. The design philosophy of the DARPA internet protocols. *SIGCOMM Comput Commun Rev* 1988;**18**:106–14.
65. Phister PW Jr, Cyberspace: The Ultimate Complex Adaptive System. *Int C2 J* 2010;**4**:32.
66. Mittal S. Cyber Complex Adaptive Systems: Methodologies, paradigms, tools and technologies. *J Defense Model Simul Appl Methodol Technol* 2015;**12**:209–10.
67. Little RG. Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. *J Urban Technol* 2002;**9**:109–23.
68. ENISA. Communication network dependencies for ICS/SCADA Systems, enisa.europa.eu 2016.
69. Ralston PAS, Graham JH, Hieb JL. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans* 2007;**46**:583–94.
70. Kotzanikolaou P, Theoharidou M, Gritzalis D. Interdependencies between critical infrastructures: Analyzing the risk of cascading effects. In: Bologna S, Hämmerli B, Gritzalis D, *et al.* (eds.), *Critical Information Infrastructure Security*. Berlin and Heidelberg: Springer, 2013, 104–15.
71. U.S. Cyber Command. Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command, 2018.
72. Kello L. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.
73. Bellovin SM, Landau S, Lin HS. Limiting the undesired impact of cyber weapons: Technical requirements and policy implications. *Journal of Cybersecurity* 2017;**3**:59–68.
74. The MITRE Corporation. Matrix: Enterprise | MITRE ATT&CK^{TM}. *MITRE ATT&CK*^{TM}, 2018.
75. SentinelOne. Eternalblue | How the NSA-developed Exploit That Just Won't Die. SentinelOne 2019.
76. The MITRE Corporation. Technique: Exploitation of Remote Services – Enterprise | MITRE ATT&CK^{TM}. *MITRE ATT&CK*^{TM}, 2018.
77. Samani R, Beek C, McFarland C. An Analysis of the WannaCry Ransomware Outbreak. *McAfee Blog*, 2017.
78. Newman LH. The leaked NSA spy tool that hacked the world. *Wired Magazine*. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ (3 July **2018**, date last accessed).
79. Langner R. To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve. LangnerGroup 2013;37.
80. Zetter K. The NSA acknowledges what we all feared: Iran learns from US Cyberattacks. *Wired*. https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/ (18 June 2020, date last accessed).
81. Rid T, Buchanan B. Attributing cyber attacks. *J Strat Stud* 2015;**38**: 4–37.
82. Nye JS. *The Future of Power*. New York: PublicAffairs, 2011.
83. Kello L. The meaning of the cyber revolution: Perils to theory and statecraft. *Int Security* 2013;**38**:7–40.
84. Obama B. Op-ed by President Obama: Taking the Cyberattack Threat Seriously. whitehouse.gov, 2012.
85. U.S. Department of Defense. Secretary of Defense Speech: Retirement Ceremony for General Keith Alexander. *Defense.gov*, 2014.
86. U.S. Department of State. Responding to Modern Cyber Threats with Diplomacy and Deterrence: Remarks Dr Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Nonproliferation, Center for Strategic and International Studies, Washington DC. United States Department of State, 2020.
87. Lin H. Attribution of malicious cyber incidents: From soup to nuts. *The Cyber Issue*, 2016.
88. Egloff FJ. Public attribution of cyber intrusions. *J Cyber Secur* 2020;**6**: 1–12.

89. Groll E. Security Firms Tie WannaCry Ransomware to North Korea. *Foreign Policy*.

90. McKeon A. WannaCry About NotPetya? *recordedfuture.com* 2017.

91. Department of Justice. Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities. United States Department of Justice, 2016.

92. Apuzzo M, LaFraniere S. 13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign. *The New York Times*. https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html (19 October, 2020, date last accessed).

93. U.S. Department of the Treasury. Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks | U.S. Department of the Treasury, 2018.

94. The United States Department of Justice. Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System, 2018.

95. Schelling TC. *Arms and Influence [Electronic Resource]*. New Haven: Yale University Press, 2008.

96. The United States Department of Justice. Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, 2020.

97. Hinck G, Maurer T. Persistent enforcement: criminal charges as a response to nation-state malicious cyber activity. *J Natl Secur Law Policy* 2020;**10**:525–61.

98. Romanosky S, Goldman Z. Cyber collateral damage. *Proc Computer Sci* 2016;**95**:10–17.

99. von Heinegg WH. Proportionality and collateral damage. *Max Planck Encyclopedia of Public International Law [MPEPIL]*, 2015.

100. Libicki MC. Expectations of cyber deterrence. *Strat Stud Quart* 2018; **12**:44–57.

101. Fishman E. How to Fix America’s Failing Sanctions Policy. *lawfareblog.com*, 2020.

102. Lin H. Escalation dynamics and conflict termination in cyberspace. *Strat Stud Quart* 2012;**6**:46–70.

103. Buchanan B. *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*. London: Hurst & Company, 2016.

104. Buchanan B. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press, 2020.

105. The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, obamawhitehouse.archives.gov 2011.

106. Department of Defense. Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, 2011.

107. FBI. Iranians Charged with Hacking U.S. Financial Sector. Federal Bureau of Investigation, fbi.gov 2016.

108. Waterman S. Clapper: U.S. shelved “hack backs” due to counterattack fears. *CyberScoop*. https://www.cyberscoop.com/hack-back-james-clapper-iran-north-korea/ (8 April 2020, date last accessed).

109. Nakashima E. Suspected Iranian cyberattack on American banks led U.S. to rally support of 120 international allies. *Washington Post*. https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html (8 April 2020, date last accessed).

110. Miller G, Nakashima E, Entous A. Obama’s secret struggle to punish Russia for Putin’s election assault. *The Washington Post*. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.858072115a9a (23 June 2017, date last accessed).

111. Isikoff M, Corn D. *Russian Roulette: The inside Story of Putin’s War on America and the Election of Donald Trump*. New York: Hachette Book Group, Inc., 2018.

112. Schneier B. *Attributing the DNC Hacks to Russia*, schneier.com 2017.

113. Baker P. How Trump’s Election Shook Obama: ‘What if We Were Wrong?’ *The New York Times*. https://www.nytimes.com/2018/05/30/us/politics/obama-reaction-trump-election-benjamin-rhodes.html (20 April 2020, date last accessed).

114. D. S Barack Obama, Neural Nets, Self-Driving Cars, and the Future of the World. https://www.wired.com/2016/10/president-obama-mit-joi-ito-interview/ (24 August 2016, date last accessed).

115. The White House. *Executive Order—Improving Critical Infrastructure Cybersecurity*. whitehouse.gov, 2013.

116. Karp BS. Federal Guidance on the Cybersecurity Information Sharing Act of 2015. *Harvard Law School Forum on Corporate Governance*, 2016.

117. Koerner BI. Inside the OPM Hack, the Cyberattack That Shocked the US Government. *Wired*, 2016.

118. Cisco Systems. *Remotely triggered black hole filtering–Destination based and source based*. cisco.com.

119. McConnell M. Mike McConnell on how to win the cyber-war we’re losing. *The Washington Post*. https://cyberdialogue.ca/wp-content/uploads/2011/03/Mike-McConnell-How-to-Win-the-Cyberwar-Were-Losing.pdf (28 February 2010, date last accessed).

120. Healey J. The implications of persistent (and permanent) engagement in cyberspace. *J Cyber Secur* 2019;**5**: 1–15.

121. Lynn WJ III. Defending a new domain: The Pentagon’s. *Cyberstrategy. Foreign Affairs* 2010;**89**:97–108.

122. US Department of Defense. Department of Defense Strategy for Operating in Cyberspace, 2011.

123. ABOUT CISA. *Official Website of the Department of Homeland Security*.

124. USCYBERCOM Malware Alert. Malware attributed to #NorthKorea by @FBI_NCIJTF just released here: https://t.co/cBqSL7DJzI. This malware is currently used for phishing & remote access by #DPRK cyber actors to conduct illegal activity, steal funds & evade sanctions. #HappyValentines @CISAgov @DHS @US_CYBERCOM. *Twitter* 2020.

125. Vavra S. Pentagon, FBI, DHS to jointly expose a North Korean hacking effort. *CyberScoop* 2020.

126. US Naval War College. *2019 Future Warfighting Symposium: Emily Goldman, Cyber Strategy and Policy*. Newport, RI, 2019.

127. Harknett RJ. United States cyber command’s new vision: What it entails and why it matters. *Lawfare* 2018.

128. Harknett RJ. Progress is the promise in national cybersecurity strategy. *Lawfare* 2020.

129. Nakasone PM. An interview with Paul M. Nakasone. *Joint Force Quart* 2019;104: 4-9.

130. Nakasone PM. A Cyber Force for Persistent Operations. *Joint Force Quarterly* 2019;104.

131. Nakasone PM. *Statement of General Paul M. Nakasone, Commander United States Cyber Command, before the Senate Committee on Armed Services*, congress.gov 2019.

132. Fischerkeller MP, Harknett RJ. *Deterrence is Not a Credible Strategy for Cyberspace (and What Is)*. Washington, DC: Institute for Defense Analyses, 2017.

133. Fischerkeller MP, Harknett RJ. Persistent engagement, agreed competition, and cyberspace interaction dynamics and escalation. *The Cyber Defense Review* 2019;267–87.

134. Barnes JE. U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections. *The New York Times*. https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html (6 June 2020, date last accessed).

135. Nakasone PM, Sulmeyer M. How to compete in cyberspace. *Foreign Affairs* August 2020; online only.

136. Maschmeyer L. Persistent engagement neglects secrecy at its peril. lawfareblog.com 2020.

137. Carson A. *Secret Wars: Covert Conflict in International Politics*. Princeton, New Jersey: Princeton University Press, 2018.

138. Nakashima E. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. *Washington Post*. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html (4 May 2020, date last accessed).
139. Nakashima E. U.S. cyber force credited with helping stop Russia from undermining midterms. *Washington Post*. https://www.washingtonpost.com/world/national-security/us-cyber-force-credited-with-helping-stop-russia-from-undermining-midterms/2019/02/14/ceef46ae-3086-11e9-813a-0ab2f17e305b_story.html (6 June 2020, date last accessed).
140. The White House. *The National Security Strategy of the United States of America*. Washington, DC: The White House, 2002.
141. Department of Defense. Summary: Department of Defense Cyber Strategy, 2018.