JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2022, 1–14
https://doi.org/10.1093/cybsec/tyac012
Research paper

Research paper

Is there a cyber security dilemma?

Carly E Beckerman *

Institute of Hazard, Risk and Resilience, School of Government and International Affairs, Durham University, Al Qasimi Building, Elvet Hill Road, Durham DH1 3TU , UK

*Correspondence address. School of Government and International Affairs, Durham University, Al Qasimi Building, Elvet Hill Road, Durham DH1 3TU. Tel: 0191 334 2257; E-mail: carly.beckerman@durham.ac.uk

Received 4 June 2021; revised 1 July 2022; accepted 24 August 2022

Abstract

In recent years, scholars, commentators and politicians have discussed the prospect of a 'cyber security dilemma'. If states race to develop superior cyberattacks, how far might this escalate? Are state-led cyberattacks likely to provoke a full war? To address these related questions, I apply a multi-level Neoclassical Realist framework that progresses from systemic logic to an assessment of leader cues and cognition. This contributes much-needed coherence to debates about escalation and cyber warfare and demonstrates the framework's utility for addressing contemporary and evolving problems in international affairs. The framework reveals that, according to both a systemic and societal cue analysis, fears regarding unchecked escalation from state competition in cyberspace to kinetic warfare are largely unfounded. Nevertheless, it also points toward one caveat and direction for further research in that cyber warfare directed at foreign leaders' political survival may be unexpectedly provocative in a way not currently addressed by escalation models.

Key words: cyber warfare, security dilemma, cyberattack, escalation

Introduction

This paper argues that there is no cyber security dilemma. This is necessary to demonstrate because an ongoing discourse exists about the potential dangers of cyberattacks and whether they alone will trigger conventional war between states. Such fears seem to be largely inspired by the language of deterrence that is used publicly among security professionals and prominent statesmen, and particularly their need to threaten rivals pre-emptively with military responses. Addressing concerns about cyber-to-kinetic escalation requires an investigation of the cyberattack phenomenon within an understanding of how inflammatory dynamics emerge. In the discipline of International Relations (IR), this context has traditionally been conceptualized as the 'Security Dilemma'.

The term *Security Dilemma* describes circumstances in which states pursue their own security with 'the perverse effect of leading to greater insecurity' because increasing one's own military prompts others to do the same [p.105, 1]. As Jervis notes, 'what one state regards as insurance, the adversary will see as encirclement' [p.64, 2]. This threat may be tangible in the sense that one state develops or purchases a new weapon that would be difficult to defend against, but 'encirclement' also has an intangible, psychological component. Changing a state's military capabilities automatically revises outside opinions about that state's motives [p.178, 3]. This is the dynamic that prompts an arms race or series of reprisals that is thought to increase the likelihood and severity of conflict. In this heightened tension, even an unintentional minor clash or misunderstanding could escalate to war [p.67, 2]. Real near-misses include the Cuban Missile Crisis of 1962 and NATO war games in 1983, but this doomsday scenario has also become part of popular culture through countless Hollywood dramatizations.

Understandably, the prospect of a 'cyber security dilemma' has also surfaced in recent years [4]. If states race to develop superior cyberattacks, how far might this new type of provocation escalate? Does 'defending forward' to deter in cyberspace only initiate mounting retaliations? Scholars at the forefront of IR have called for more research, asking, 'If I do take a more offensive posture in this domain, what does it do? That's a critical question' [para.16, 5]. Indeed, the risk of escalation from cyberspace to conventional warfare is being recognized as 'a crucial area of policy-relevant research' [p.2, 6]. In response, I argue that the systematic multi-level analysis provided by a Neoclassical Realist (NCR) framework contributes much-needed coherence to debates about escalation from cyber warfare to conventional military clashes between states. Using this framework, I explain how unchecked escalation towards a cyber security dilemma

would defy the structural logic that informs most security strategy and run counter to theory-informed expectations of deviant state behaviour. It should, therefore, be treated as a highly unlikely eventuality. This is not a prediction so much as a plea to move beyond catastrophism and recognize that the so-called 'cyber security dilemma' and related phrases such as the 'cyber arms race' are red herrings that distract from other potentially more useful research agendas.

As such, this article makes two related contributions. First, it provides a more developed and theory-driven analysis of cyber warfare between states as normal and expected behaviour. This means that this particular paper is not concerned with escalation *within* cyberspace, from, for example, espionage to sabotage, or activities that only reflect the interests of non-state actors. This narrow focus is necessary to answer the specific fears of a security dilemma and also underscores the need to move beyond a grand theory of cyber warfare as unrealistically complex. This is discussed more below. Second, the paper provides clear insights that actively extend, systematize and ultimately reinforce some earlier arguments introduced by a subsection of scholars, most notably Rid, Liff and Singer and Friedman [7–9]. For example, although Jensen and Valeriano have acknowledged that cyber capabilities can offer states the option to de-escalate international conflicts, using a coherent NCR framework demonstrates why such 'offramps' and 'firebreaks' are reassuringly automatic [p.2, 6].

The rest of this article proceeds in five parts. It explains how the desire for deterrence in cyberspace is creating fears of a Security Dilemma. Then it demonstrates why this problem benefits from an NCR perspective. Next it invokes a purely systemic Realist logic and argues that states appear unlikely to escalate tensions with their adversaries based on cyber capabilities alone. This is because cyberattacks fail to reveal the extent of a rival's abilities or their full possible range of intentions, meaning that states cannot specifically balance against cyber capabilities alone and so are not faced with a *new* arms race. The paper then incorporates a boundedly rational perspective informed by the cognitive turn in post-Cold War Foreign Policy Analysis (FPA). This analysis indicates how the interplay between material conditions, societal contexts and leader decision-making also suggests that cyberattacks are unlikely to be responsible for new tensions.

The final section then offers an illustrative case study of the Shamoon attack in 2012. At the time of writing, there have been no examples of cyber-to-kinetic escalation between states. This prevents a controlled comparison or test of deviant cases. Shamoon provides an excellent illustration because these incidents took place between two powers who are not only engaged in ordinary rivalry but also high-tension, high stakes competition that spans from security and existing proxy conflicts into multiple economic and ideational issues fed by a troubled shared history and external intervention—this type of scenario naturally generates concerns about escalation. The fact that, despite this atmosphere, Iranian cyberattacks did not prompt a degenerative spiral, makes Shamoon a key example. This case study demonstrates how, even under provocative geopolitical conditions, highly invasive cyberattacks between rivals function alongside state competition without escalating it to the physical domain. Based on this multi-level framework and illustrative case, I argue that—while cyber warfare exists—there is no incendiary cyber arms race and no cyber security dilemma.

The novelty of this field means it is also necessary to make a brief note about definitions. I adopt *cyber warfare* as a catch-all term to refer to state-orchestrated surveillance, espionage and sabotage efforts in cyberspace that attempt to breach the confidentiality, availability and integrity of networks and systems that are valuable to foreign states. As such, there is no need to distinguish between computer network exploitation (CNE) and a computer network attack (CNA) when discussing hypothetical escalation. The term *cyberattack* might refer to individual stages within specific operations, or it might refer to a single code-named operation as a whole. This article does not consider *cyber war* to be a stand-alone concept as this scenario has been widely debunked [10]. That term is not used. Following the example of Schneider, information warfare orchestrated online is treated as a separate phenomenon because it involves attempts to manipulate foreign publics rather than breach protected networks [11].

Expectations of a Cyber Security Dilemma

Initially, it is necessary to establish that fears regarding unchecked escalation from cyber to conventional warfare are entirely understandable. Governments that openly pursue deterrence in cyberspace seem to be accepting the possibility of violent escalation with an ease that is concerning to many observers. Although the burgeoning literature on cyber warfare has provided arguments to the contrary, that literature has struggled to address state-to-state escalation cohesively. These points are developed below.

This paper is concerned with the public discourse that is alarmed about cyber deterrence, and the fear apparent among observers who equate government attempts to deter in cyberspace with an unchecked spiral towards traditional war. When discussing cyberspace, deterrence is generally equated with punishment in the form of decisive retaliation. The aim is to discourage potential attackers by making their associated costs unreasonable on an ongoing basis [p.56, 12]. General James Cartright, for example, who initiated much of the USA's cyber strategy, said after he retired that 'we've got to talk about our offensive capabilities […] so that people know there's a penalty to this' [para.2, 13]. The same sentiment was echoed by Admiral Mike Rogers as head of the National Security Agency (NSA) and United States Cyber Command (USCYBERCOM) under Presidents Obama and Trump [14]. This is why the Pentagon created a task force on cyber deterrence focused on ways that the USA might 'hurl back' in cyberspace [para.5, 14]. President Trump rarely commented on cyberattacks, but he specifically mentioned reprisals against Iran, insisting that 'If we ever get hit, we'll hit very hard. We'll be able to hit very hard' [para.3, 15]. As president elect, Joe Biden likewise threatened to impose 'substantial costs' on adversaries targeting the USA through cyberattacks [16].

Although it is unlikely that threat-based deterrence is possible against small-scale incursions, articulating a commitment to retaliation is intended to avoid the appearance of weakness and the steady erosion of credibility that can result from inaction [2]. The prevailing logic dictates that states attempting to protect themselves and prevent war must always appear willing to wage it. This is why the US Department of Defense announced that it intends to counter all cyberattacks, even minor intrusions, 'including activity that falls below the level of armed conflict' [p.2, 17]. US officials are apparently even willing to use conventional, kinetic weapons in response to severe cyberattacks, and intend to deter the most crippling form of cyberattacks with threats of nuclear retaliation [18]. Indeed, cyber warfare is often discussed as though it has a nuclear weapons-level of importance to strategic planning. The Cyberspace Solarium Commission (CSC), for example, noted the importance of a cyber second-strike capability, 'to ensure that we can reconstitute in the aftermath of a national-level cyberattack' [19].

The expected spiral of retribution has worried observers for many years (see, for example, [20–30]). The former Secretary of Energy,

Ernest Moniz, called threats of cyber reprisals 'a very fundamental step in the wrong direction' [para.4, 31]. There is a general feeling that 'cyberspace has opened up a new sphere of activity […] taking us closer to the threshold of an armed attack' and 'new escalatory risks' [para.4, 32]. Maurer has noted that 'states around the world have not yet learned how to interpret signalling in cyberspace, creating uncertainty, potential for misinterpretation and novel risk for escalation' [para.4, 32]. As such, some commentators are convinced that 'an arms race in cyberspace' is underway [para.29, 31]. Much of the formative work on cyber escalation has begun with this premise, that the intensification of hostilities from cyberspace to the material world is both possible and likely (see, for example, [33–37]). A 2021 book highlights this prevailing discourse in its title: *This Is How They Tell Me the World Ends: The Cyber Weapons Arms Race* [38].

Scholars of cyber warfare have shown little interest in addressing these fears of deterrence policies by situating cyber escalation within theories that deal with the conduct of competitive IR as a whole. This is not an oversight so much as an unintended consequence of scholarship that is responsive to strategic priorities. Theorizing on the nature of cyber conflict in general will encompass not only state interactions, but also non-state and criminal activities with blurred distinctions between those categories. This need to address multiple forms of conflict at once has left the specific and narrower question of 'is there a cyber security dilemma?' as one small component of most existing work. State interactions in cyberspace lend themselves to the application of established IR theories. However, it has seemed artificial to address only state interactions, which has unfortunately allowed confusion regarding those state interactions to persist. As Healey and Jenkins [39] note, 'supporters believe these [deterrence] actions should significantly reduce attacks against the United States, while critics worry that they may incite more adversary activity. As there is no standard methodology to measure which is the case'.

In response to the specific question of escalation from cyber to kinetic warfare, most of the existing literature has unofficially delivered a Classical Realist approach—offering wisdom for a series of self-contained scenarios. Martin Libicki's detailed early RAND study on *Crisis and Escalation in Cyberspace* (2012) falls into this category, as well as Jasper's more recent *Strategic Cyber Deterrence* (2017), Kostyuk et al's 'Determinants of the Cyber Escalation Ladder', Whyte and Mazanec's *Understanding Cyber Warfare* and Valeriano, Jensen and Maness' *Cyber Strategy* [37, 40–43]. This scholarship offers clear arguments against catastrophic thinking, but for individual situations rather than as rules of state behaviour. Due to the perceived necessity of commenting on multiple forms of cyber conflict at once, uses of theory have been restrictive, with scholars relying on Kahn's (1968) escalation ladder or the principal-agent model (see, for example, [44, 45]). This may be why Jervis has remarked that escalation ladders are 'poorly understood' and 'quite unclear' in the cyber realm [p. 73, 46]. I argue that a new application of established theory is needed here, 'to clarify concepts and ideas that have become, as it were, confused and entangled' [p.132, 47].

The Need For a NCR Framework

The nature of cyber warfare as a topic means that the term can refer colloquially to many state and non-state phenomena at once that may fluidly transition between categories, from surveillance and espionage to weapons of mass destruction, the spread of misinformation and even the online activities of terrorist organizations. This fluidity means that it is proving unrealistic to try and conceptualize the escalatory problems posed by all of these activities within a single grand theory. This realization—that grand theorizing is not always fruitful—is well-established within IR, prompting the development of many mid-level frameworks that address real-world problems more effectively by separating them into constituent components [48]. For example, the efficacy of this piecemeal practice led scholars to abandon the frustrating search for a grand comparative theory of foreign policy as early as the 1970s [48]. Given the inherent fluidity of cyberattack phenomena, efforts to develop a grand theory of cyber escalation are, as discussed above, proving similarly stunted.

As such, this paper adopts a compartmentalized approach, in which some key concerns associated with cyber warfare might be isolated for study to identify whether a causal pathway is likely to exist between a specific phenomenon, in this case cyber warfare between states, and the concerning potential outcome of conventional warfare between states. The paper answers a widespread public fear that such a pathway exists, thus providing a deliberately narrow contribution. Instead of trying to pre-empt all specific cyberattack situations, it is far more useful to ask whether cyber warfare can escalate as one very specific question about state and governmental behaviour in the general confines of the current international system. This requires a framework capable of defining a set of rules that might be useful to practitioners, but which also serve as a coherent basis for debate and revision. The multi-level approach permitted by Neo-Classical Realism is particularly useful for these purposes. This section explains the ethos behind NCR and how the framework for this article has been derived.

As the heir to Classical and Neorealism, NCR allows for a layered framework to interrogate the interplay between these different levels of analysis [49]. This means that, in order to explain any foreign policy case or phenomena, NCR frameworks must untangle the role played by systemic prompts and constraints but also pin-point which unit-level variables are intervening within that structural context [50, 51]. Rather than parsimony alone, the aim is to develop a realistic illustrative model that follows the precedent set by Labs, Yordan, Schmidt and Toft in rejecting any analytical demarcation between theories of international politics and theories of foreign policy [52–55]. This is because focusing only on systemic variables or only on societal factors leads to frameworks that are 'sorely deficient' for appreciating the complexity of global politics [p.298, 56]. Indeed, Nygren calls for more NCR interpretations specifically because a sole 'focus on resource developments often results in worst-case scenarios' [p.518, 57].

Although it can be very difficult to discern and justify the differentiation between international versus domestic variables in historic cases, this article benefits from a long-running tradition within the study of escalation, of transitioning from a systemic analysis to a psychological assessment of leaders and governments [2]. Procedurally, I derive a multi-level framework in keeping with this approach.

The initial systemic assessment reflects core assumptions about state behaviour, all of which rest on the implications of rationality under conditions of anarchy [p. 58, 2]. In the absence of an overarching authority, all states must compete to maximize their relative power to facilitate survival [58; pp. 60–61, 59; p. 3, 60]. This outlook largely relies on the simplest definition of power as tangible assets rather than as the ability to coerce [p.55, 58]. Power may also be tangible but latent, meaning that population size and wealth provide resources for enlarging the armed forces [pp.60–61, 60]. The Realist tradition also includes more nuanced understandings of power, including Nye's distinction between hard, soft and smart varieties, but these terms are descriptive and prescriptive, rather than means of

modelling state behaviour, and so are less relevant here [61]. Rather, states are assumed to be primarily concerned with the distribution of power in the international system and will balance against their adversaries' material capabilities [p.15, 62; p.36, 60; p.73, 63; p.4 64]. Whereas Offensive and Defensive Realists disagree on how aggressive states must be to survive despite anarchy, all approaches require that states be able to compare their capabilities. An awareness of this power distribution 'does not try to predict particular wars, but the general propensity to war' [p.7, 65]. Evaluating cyber warfare through this lens aims to identify the broadest trends and explanations for what we can observe and expect. This is the base line.

Such a structural analysis also addresses cyber warfare in a language and logic familiar to national security practitioners, principally because cyber warfare between states occurs under conditions of limited information and within a perceived context of perpetual competition and suspicion. Attempting to bypass this heavily embedded worldview has a tendency to invite scorn from government strategists. Former National Security Advisor and influential political commentator John Bolton, has, for example, been particularly dismissive of any criticism directed at American aggression in cyberspace [66].

At the structural level, Neorealism focuses on systemic constraints that provide general guidelines of expected state behaviour. Neorealism does not view structure as inherently causal or inescapably constraining. Instead, 'systemic pressures and incentives may shape the broad contours and general direction of foreign policy without being strong or precise enough to determine the specific details of state behavior' [p.146, 67]. When this ideal-type behaviour does not occur, Realist scholars generally expect that the deviance was caused by an interruption or intervention from some form of sub-state phenomena [50]. This means that the intervening variables that most often concern NCR research are related to 'mistakes and maladaptive behavior' [p.294, 50]. As Rathbun notes, 'The state is still present, only overcome' [p.296, 50].

Then what are the intervening variables when questioning the existence of a cyber security dilemma? The Security Dilemma is thought to occur when it is not possible to distinguish between an adversary's defensive or aggressive intent [p.199, 3]. In the traditional structural framework, state intentions are inferred from signals such as military build-up and unilateral disarmament. However, when this type of signalling cannot be produced, it is necessary to address intent at the psychological level. Focusing on systemic factors must adopt an ideal form of rationality in which state behaviour is expected to maximize utility; studying psychological issues reflects an awareness that, in human leaders, rationality is bounded [68].

This awareness of bounded rationality is championed by the field of FPA. FPA refers to the study of foreign policy decision-making, specifically the point of intersection between material and ideational factors. Rather than assuming that the point of intersection is the state, FPA's main unit of analysis is human decision-makers [48]. FPA is rooted in Classical Realist perspectives but developed alongside Neorealist-dominated IR throughout the second-half of the 20th century. As a result, FPA offers a range of useful models to investigate and theorize sub-state causal pathways within the structural constraints identified by a Neorealist worldview. The emergence of NCR has then explicitly provided for the harmonizing of Neorealism and FPA to form a 'coherent logic' by building layers of analysis [p. 296, 50, 69, 70]. When considering escalation out of cyberspace, and based on an accumulation of FPA research, I address how leaders are expected to respond to material contexts, trends in societal attitude formation and political priorities. After a structural assessment of constraints, these three influences represent the intervening variables for this study and are expanded in detail below.

Cyber Power and Barriers to Escalation—A Structural Assessment

Structural Realist logic allows several key assertions about the limits on escalation from cyber warfare. Crucially, cyberattacks do not indicate capabilities or future intent. This means that cyber capabilities do not alter the distribution of power and so do not create a *new* arms race, while traditional military deterrence and systems of signalling prevent the use of cyberattacks so violent that they would clearly be acts of war. These points are elaborated below.

First, it is impossible to measure cyber power in isolation. In an information environment, there are three traditional security goals referred to as the CIA triad: confidentiality, integrity and availability [p.35, 9]. Attacking confidentiality simply means intercepting valuable private information, sensitive data and communications. If a system is penetrated, an effective attack on its integrity means the system can be changed without authorization [9]. Attacking availability successfully then means that a target loses normal use of its systems [9]. When considering conflict interactions, cyber capability would primarily reflect a state's ability to complete these types of operations against targets that are valuable to an adversary. Such a capability is impossible to measure without referring to a range of cumulative potential indicators such as budget, command and control capability and scale of their digital economy [71]. Whereas traditional military equipment such as fighter jets, battleships, tanks and manpower are visible and quickly translatable into an estimate of material power, cyber capabilities are invisible, intangible and may be constantly changing.

This puts intelligence agencies at a disadvantage. The American Central Intelligence Agency (CIA) can notice foreign interference, such as clandestine Russian social media influence operations in 2016. It can also monitor certain personnel performing hostile acts online, such as the indicted officers from PLA Unit 61398 in China. Likewise, Finnish authorities might notice suspicious disruptions in their GPS signals, and the Dutch government can prosecute Russian cyber experts after a thwarted attack on the Organization for the Prohibition of Chemical Weapons [72, 73]. Nevertheless, there is no offensive foreign equipment that these intelligence agencies might quantify for immediate reassurance about any changes in the distribution of cyber capabilities. This is true even in the strictly military sphere.

While it is becoming standard practice for states to integrate increasingly sophisticated technology into their conventional forces, cyber capabilities can only be used to increase the effectiveness of traditional militaries, not their size. It could be possible to infer how much government spending is directed towards offensive cyber operations in the national budget, but there is no asset to count. There are no silos, no cyber stockpiles for other states to notice and balance against. There are some well-known training games, such as workshops run within the EU and NATO, but generally there are no cyber military manoeuvres to monitor either. This means that the term *cyber power* cannot refer to the physical equipment involved in pursuing state security in cyberspace. To calculate relative power, there needs to be an observable ratio of capabilities between defender and challenger [74]. An isolated assessment of any foreign state's offensive cyber capabilities simply defies this type of measurement.

Knowledge of existing cyberattacks also fails to provide enough comparative information. The term *cyberattack* could refer to a single

stage of the 'intrusion kill chain' or the entire seven stages (reconnaissance, weaponization, delivery, exploitation, installation, command and control and actions on objective) collectively [75]. A successful attack might have temporary or permanent effects. It might be a single or cumulative attack and have immediate or long-term consequences. It might leave no trace or be physically destructive, and it might be obvious or go unnoticed by the adversary for a long period of time. All of these outcomes depend on the target chosen, type of operation conducted and ultimate goal. The number of possibilities is incalculable, which prevents existing cyberattacks being relied upon as a definitive measure of cyber power.

Although it is reasonable to assume that all states with militaries also possess some form of offensive cyber capability, it appears neither possible nor optimal to balance against only the cyber component. No state would ignore a large increase in adversaries' arms purchases to focus only on their uncertain ability to infiltrate networks. The traditional calculation of relative power remains a *modus vivendi*. Cyber capabilities do not change this particular equation.

Importantly, the opacity of these weapons also means it is impossible to judge whether any cyber capabilities exist mainly for offensive or defensive purposes [3]. Although multiple scholars, such as Saltzman, Gartzke and Lindsay, as well as Slayton, have addressed offense-defense theory with regard to cyberspace, these discussions have focused on the optimal ratio for military planners working with full information [23, 26, 76]. It is acknowledged that even if two adversaries deploy a cyber weapon, there is no way to perform a comparative net assessment and compare the offense/defence balance before and after.

Even if cyber power was separately quantifiable, it would be a poor indicator of future intentions. This is because cyber weapons cannot be stored for later use and because no single attack or collection of attacks can definitively indicate the nature and specific target of future attacks. Whereas ballistic and incendiary weapons can ostensibly damage any undefended target, the same is not true for cyber weapons. States' cyber capabilities are useful for exploiting vulnerabilities. Most often, this means that the only cyber weapons worth balancing against would be time-sensitive and single-use anyway, relying on zero days. The traditional Minuteman intercontinental ballistic missile (ICBM) originated in the 1950s and still protects the USA, but cyber weapons are rendered inert as vulnerabilities are discovered and patched [pp.168–169, 7]. This can be achieved in a matter of minutes. Increased sharing of information, such as USCYBERCOM's 2018 decision to upload samples of malicious malware to VirusTotal, further limits the shelf life of cyber capabilities [10]. These realizations are important because it is concern over what happens next that triggers escalation. If there is no way of understanding the full extent of adversaries' capabilities, then attempting to balance against them is impossible.

Instead, ongoing limited-scale cyber warfare reflects Realist expectations of state competition. In 2019, General Nakasone of USCYBERCOM informed the Senate Armed Services Committee that 'cyberspace is a contested environment where we are in constant contact with adversaries' [77]. Particularly, he focused on sustained Russian and Chinese campaigns that function below the level of armed conflict but are designed to erode American power. Such activities are mutual, of course. As former Deputy Secretary of Defense Robert Work noted jovially on the subject, 'If you ain't cheating, you ain't trying' [para.18, 14]. None of this rivalry reflects an inadvertent spiral.

Through this lens, American and Russian attempts to hack each other's national electric grids are normal and almost good practice [78]. Both powers maintain a conventional second-strike capability, and both ensure that their ICBMs are capable of hitting the other's major cities. All major powers have reportedly developed ways to target their rivals' key economic systems, infrastructure, financial markets and transport networks, making the Trump administration's seemingly drastic plans for nuclear cyber deterrence, oddly ordinary. Instead of a new or additional arms race in (or because of) cyberspace, there may be a kind of bureaucratic contest over pouring research and development resources into designing new capabilities. The largely invisible results of this expenditure also inhibit a spiral of balancing. Even if rivals responded to cyber competition in the material world by sponsoring hostile proxies such as terrorist organizations or domestic opposition groups, this would also be indistinguishable from traditional *Realpolitik*. Cyberspace does not alter the pre-existing dynamic.

Limited but persistent cyberattacks and retaliations may also appear threatening because they endanger a state's democratic or economic future, but escalation to kinetic war would have to be on purpose rather than part of a downward spiral. There is a variable amount of risk that must enter the adversary's calculation. If the intent is to compete below the threshold of war, then state-led cyberattacks will deliberately exercise restraint to avoid conventional retaliations. If the intent is to initiate or participate in kinetic warfare, then the Security Dilemma problem has become redundant. Only states that have the necessary military hardware for actual shooting wars would opt for this course of action, again reducing the question of cross-domain escalation to one of basic hard power comparison. States may wish to enter conflict, but the existence of cyber warfare does not increase their propensity to escalate.

Recent research supports this assertion. During wargames, Schneider found that American participants from the US government overwhelmingly refrained from using destructive cyberattacks until after conventional conflict had already begun [11]. These games were designed to reflect the rise in US cyber capabilities between 2011 and 2016, but there was no corresponding increase in the offensive use of cyber capabilities during those years. During Schneider's simulations, fears of cyber escalation led to 'tight rules of engagement' [p.32, 11]. This suggests that competition and in-kind retaliation is perceived as acceptable, but escalation to conventional warfare is deliberately avoided. Indeed, there are only two known instances when states have used kinetic force in retaliation for cyberattacks. The first was an American drone campaign against the Islamic State in 2015 and the second was an Israeli airstrike on Hamas cyber operatives in 2019 [10]. In both of these confrontations the use of conventional force was technically an escalation, but both targets were non-state actors and so there was no meaningful danger of initiating the Security Dilemma and accidentally triggering a spiral towards war.

Even controversial cyberattacks have not directly provoked kinetic responses. Iranian retaliation for Stuxnet has been confined to hacks such as Cleaver, Newscaster and Shamoon. In turn, the Saudi response to multiple Iranian Shamoon cyberattacks against its oil and corporate networks in 2012, 2016, 2017 and 2019 has been inward, with more focus on cybersecurity [79]. Similarly, Israel and Iran traded serious cyberattacks on CNI targets in April, May and June of 2020 with no new escalation to weapons outside of cyberspace occurring because of these attacks [80]. Likewise, the 2020 Solarwinds attack that compromised 'dozens of incredibly high-value targets' within US government agencies (for which Russia is tacitly held responsible) provoked no knee-jerk reaction [81]. As restraint continues to be exercised, this should also help to signal a lack of aggressive, escalatory intent [p.373, 82].

Does that mean that seeking deterrence in cyberspace is pointless? Rather than aiming to punish, it seems that developing 'deterrence by denial' is key [83]. Patriotic or criminal cyberattacks might be carried out by persons affiliated to or even directed by state authorities, but punishing those individuals will not deter the state itself. Instead, the 'pest' scale of attack has been countered using a combination of retaliatory hackbacks and vigilance. The aim of this tactic is to simply deny the adversary any benefit so that an attack becomes futile [p.54, 84; p.37, 60]. Deterrence is achieved if attackers refrain because they expect failure [p.112, 41]. Valuable information might be protected, for example, by populating a system with thousands of subtle decoy files that can only be differentiated by their genuine owner [85]. Groll has complained that this indirect deterrence strategy is 'a lot harder than it looks and a lot less rewarding than it seems', but the costs associated with conventional conflict would be far higher [para.46, 86].

Therefore, the prospects do not seem bleak. Cyberattacks cannot be used to gauge capabilities or future intent, meaning that states cannot specifically balance against them or create a new arms race. This renders an inadvertent spiral of escalation from cyberspace into kinetic violence decidedly unlikely. The following section also addresses the role of human decision-making.

Cyber Threat-Perception and Barriers to Escalation—A Sub-State Assessment

In the absence of definitive signals (such as military build-up) that serve as hard evidence, states' assessment of each other's intentions must be occurring without clear evidence, i.e. involving biases and heuristics. Does considering human cognition cause us to revise the likelihood of a cyber security dilemma? There is no consensus on how threats are formed in the mind, so it is reasonable to see any decision to escalate as a culmination of interplay between material contexts, societal contexts and personal cognition [87–89]. I combine these sub-levels of analysis to make one assertion about escalatory cyber warfare and add one caveat: the existence of cyberattacks does not alter pre-existing biases used to gauge adversary intent, which means that a spiral of escalation from cyber to kinetic warfare remains unlikely; however, under specific conditions, cyberattacks also represent a new form of signalling that risks misinterpretation. These points are discussed below.

As it is not possible to measure cyber power in isolation, some relevant data for considering material contexts is missing. However, it is possible to gauge traditional measures of power, such as military and economic capability, geography and population size, as well as understand existing state interactions (hostile and friendly), and know some facts of existing cyberattacks. An analyst armed with only these details should view deterrence favourably because simply amassing capabilities involves low cognitive effort [90]. The need for deterrence seems more obvious as a security situation worsens, such as when there is a noticeable increase in the adversary's military build-up or a rise in detected cyberattacks. Striving for superiority under these conditions drives up defence spending [91]. However, in the absence of certainty regarding any adversary's comparable cyber capabilities, a strategy of deterrence translates simply into more spending on technical research and development and a focus on monitoring and ejecting intruders. This type of internal development and limited retaliation, as noted above, is also largely invisible to outside observers. It cannot prompt an arms race.

In contrast, the decision to escalate after incurring cyberattacks is an attempt to re-establish lost deterrence. This is an entirely different activity that is closer to compellence: trying to compel an adversary to adopt a specific behaviour. However, pursuing compellence is complex, non-specific and ongoing, shining an uncomfortable spotlight on (almost inevitable) short- or long-term failure. Such a purposeful strategy requires unattractively high cognitive effort, rendering escalation from cyber to kinetic warfare cognitively unattractive in light of the material conditions alone [90].

Is this still the case when we consider the interplay between material and societal factors? Whether an adversary is viewed as a threat, and whether action against them seems plausible, are considerations shaped by societal cues [92, 93]. Constructivism and developments in securitization theory have demonstrated how threat perception has discursive communal origins, reflecting and reinforcing identities and narratives that may also be manipulated (see, for example, [94–96]). For one nation to view another as threatening requires an often indistinguishable mixture of these group sentiments and observable conditions [93]. In the throes of a pandemic, for example, Italian polling showed a surprising shift in public assessment of Russian, Chinese and German hostility based only on how those governments responded to Italian pleas for healthcare aid [97].

Usefully, although these are sentiments rather than concrete calculations, they are also relatively uniform within groups. Societies often possess a collective sense of who their foreign adversaries are. Chinese university students, for example, intuitively report that the main threats to China are the USA and Japan [89]. British polling in 2019 highlighted Russia, China, Iran and North Korea as the main threats [98]. Indians consistently rate Pakistan as the nation's biggest threat [99]. These are all unsurprising answers—no one is concerned about New Zealand.

This is because trends in the interactions between two or more states frame each society's expectations about how threatened they would feel in the event of conflict. Technologically advanced states such as Estonia and Canada do not seem threatening in cyberspace because they have not been engaging in conventional security competition. The result can be summed up as a bias in threat perception termed *subjective credibility* [100]. Once entrenched, it is highly resistant to change [p.4, 100]. The cognitive expense of re-evaluating security threats is very high, and humans often prefer to misinterpret challenging information rather than revise established beliefs [100].

In the absence of definitive data regarding relative cyber capabilities, whether another state feels threatening in cyberspace must be determined predominantly by subjective credibility. There is a group 'sense' of threat rather than any purely objective computation. Crucially, this means that strategists are not faced with an unpredictable array of new adversaries. The USA, for example, does not have a cyber warfare problem so much as it has a China/Iran/North Korea/Russia problem. The securitized nature of relations with each of these states is well-understood in American strategic planning. This familiarity should limit fears about the likelihood of catastrophic error occurring through overstretch or overkill, reinforcing Liff's earlier observation, that ''cyberwarfare' will usually occur in the context of a larger political, strategic interaction…' [p.135, 8].

Consider attribution. Whereas the development of clear and consistent cyberattack attribution mechanisms is important for law enforcement, subjective credibility makes attribution far less problematic for states competing in cyberspace. As adversaries engaging in cyber warfare are already entwined in other forms of security competition, the likely perpetrators are not difficult to list. An advanced persistent threat (APT) directed at Ukraine, for example, would have one obvious suspect. Indeed, this was a key part of the reasoning that led analysts at Symantec to attribute the Stuxnet worm tentatively to Israel and the USA before it was confirmed by leaked documents—

these actors had the clearest motive amid their decades-long shared history of antagonism [101].

These societal biases also reflect implicit preferences that influence the ontology, or worldview, of state leaders [p.740, 102]. Causal beliefs about how A leads to B in international politics, as well as normative beliefs about whether those actions and outcomes are good or bad, coalesce to define the realm of possibility for all foreign policy actions [p.741, 102]. During a crisis, particular details will trigger the relevant parts of this culturally embedded ontology. Societal cues reflect the psychological environment in which leaders make decisions [103]. Crucially, within the most cyber warfare-active states, these ontologies do not seem to tolerate the prospect of escalation to kinetic attacks. Studies by Kreps and Schneider, as well as Jensen and Valeriano, have found that general publics in the USA, Russia and Israel do not equate cyberattacks with conventional military strikes, and so they do not favour escalation from the former to the latter [6, 17]. These are all nuclear powers, so each societal ontology includes an implicit acceptance that conventional military escalation is possible. While their attitudes towards cyber warfare are not binding and cannot be assumed to be universal, their distinction between domains and rejection of cyber-to-kinetic escalation should be cause for optimism.

There is one remaining problem. It is not the material conditions or societal cues that really worry outside observers. What if decision-makers are volatile, unpredictable or unreliable? Those with less advanced cognitive skills, for example, tend to respond emotionally to perceived attacks and react with heightened competitiveness [104]. Unfortunately, it is very difficult to articulate blanket rules about how individual cognition affects behaviour on the international stage.

Keller and Yang, for example, sum up four elements of leader cognition (military assertiveness, distrust of others, belief in ability to control events and self-monitoring) that help politicians translate material and societal cues into specific options for dealing with a crisis [102]. These categories operate on wide spectrums that defy easy generalization. In addition, some research suggests that national leaders are likely to ignore material contexts altogether and judge adversary intent based on personal theories [100]. Even politicians' feelings about particular situations, while sometimes demonstrating signs of 'performative emotional cues relevant to the state', can also reflect individual sentiments with little relevance to the people they govern [p.1235, 105]. It is clearly inadvisable to assume that all leaders will respond to cyberattacks in the same way.

To appreciate the importance of any dangerous impulsiveness, it is necessary to anticipate (A) when a leader's ontology may be disconnected from constraining societal norms, while (B) that leadership is cognitively under-developed, and (C) the triggering conditions for their decision to escalate. Items (A) and (B) are likely indicated by a leader's rhetoric and previous responses to threat. However, generalizing any principles for item (C) requires a keystone variable that is close to being universal among national leaders, regardless of their individual traits.

I posit that this lowest common denominator is the primacy of political survival. Cognitive research on foreign policy decision-making considers leader deliberations to be nonholistic or nonexhaustive, dimension-based, satisficing, order-sensitive and noncompensatory [106]. This means that politicians consider only a truncated range of options, which are clustered into organizing themes. They eliminate options according to their basic requirements rather than actively searching for an optimal alternative; their preferences are affected by the order in which they receive information, and they have some basic requirements that cannot be compensated for. Assuming that political actors operate under self-interested motivations, politicians see gains and losses first in terms of their political position and only afterwards in the context of national interest [107, 108]. This reflects a noncompensatory loss-aversion principle. Options that threaten the leader's political survival are abandoned immediately, truncating the range of available alternatives [p.84, 106].

This impacts our understanding of cyber warfare in two ways. On one hand, cyber warfare offers decision-makers an attractive array of politically low-risk options to continue the practice of politics by other means [23]. However, cyberattacks could also be a medium of inadvertently aggressive signalling if they target a foreign leader's political survival. This is discussed below.

Cyberattacks can be conducted quickly and clandestinely to avoid scrutiny, or publicly as part of a long-term strategy that is demonstrable to the leader's base. Denials may be issued, but also 'non-denial denials' that deliberately prevaricate [109]. The target may not know that it has been subject to cyber warfare for many months, inherently constraining their options once the intrusion is discovered. Additionally, without an obvious incoming projectile, the target is under no obligation to admit that an attack occurred. This provides political cover for any concessions, meaning that cyberattacks can help to incentivize cooperation without hardening opposition. The Stuxnet worm was an ideal example: bombing Iran's nuclear facility at Natanz would have precluded any Iranian participation in negotiations. The use of malicious code did not. Wielding cyber warfare as a tool of security competition should, therefore, present less risk to all parties' political survival than conventional strikes. Even among performatively hawkish leaders, limiting retaliation to cyberspace should be preferable.

Nevertheless, a particular leader's sensitivity to political risk is highly variable. Following the logic of the noncompensatory loss-aversion principle, if a leader perceives that cyber warfare is being used directly or indirectly to undermine their regime, and the risk to that survival crosses a certain threshold, then escalation may become their least risky or only viable option [110]. This might be an unintended outcome of information warfare online and the attempt to influence a foreign leader's base, or it may stem from cyberattacks conducted in a similar manner to targeted sanctions that strip the personal wealth of regime loyalists. To create a dangerous situation, the target state or government would need to feel in danger of toppling, and they would need to perceive that this outcome would be the result of a particular adversary's deliberate cyberattacks. Therefore, as politicians are motivated in the first instance by a desire to protect their political survival, cyberattacks that seriously threaten an individual foreign leader's career or position may be unexpectedly provocative, even if they are far below the threshold of war.

Such a provocation may be entirely unintentional. This is because the psychological impact of cyberattacks on calculations of political risk could easily be greater than usual. Propaganda is normal, but information warfare can often seem like a violation; the attempt to turn elites or the public against a particular leader through social networks accessed on personal devices feels invasive and pernicious [111]. Whyte demonstrates a less extreme version of this dynamic in American responses to Russian electioneering in 2016 [112]. Similarly, targeted sanctions are commonplace, but using cyberattacks to confiscate wealth could be far quicker than even the harshest of sanctions, providing more impetus to respond. As the level of tolerable risk is different from leader to leader, it is difficult to know in advance how far these otherwise non-destructive attacks can be allowed to go. Some authoritarian leaders in particular have been diagnosed at a distance with narcissism and paranoia that would play a role in their political threat perception [113].

Differences in how adversaries view the cyberspace–political survival relationship are already apparent in Russian and Chinese statements. Responding to American calls for freedom of speech online, both governments have equated the spreading of unflattering news via social media with something as serious as cyberattacks on powerplants [114]. The notion of *attack* is relative to the risk it presents to regime survival. Although it should not be surprising that attempted regime change is provocative, the recognition that cyberattacks may be unintentionally interpreted as attempted regime change should provide pause for thought.

Case Study: Shamoon 2012

The multi-level NCR-based argument presented in this paper indicates that escalation from cyber to kinetic warfare should be treated as a highly unlikely eventuality. In a structural analysis, cyberattacks do not indicate the extent of capabilities or future intent, meaning that states cannot specifically balance against them or create a *new* arms race. At the state level, an awareness of how material and societal contexts influence leader decision-making reinforces this assessment. While it is not possible to test a deviant case or conduct a controlled comparison (as noted above, there have been no incidents of cyber-to-kinetic escalation between states at the time of writing), this section offers a structured narrative of the 2012 Shamoon attacks as an illustrative case.

Shamoon is a pertinent case because there remain lingering fears about the possibility of escalation from cyberattacks to kinetic warfare when discussing the Middle East. Kausch, for example, argues that 'the political use of cyber tools works as a powerful accelerator of geopolitical confrontation in the Middle East' where existing tensions 'gain an additional arena for much faster escalation' [p.7, 115]. Likewise, Baezner asserts that 'Tit-for-tat actions in cyberspace and in the physical realm increase risks of misperception in cyberspace and escalation of the situation into open conflict' [p.18, 116]. Shamoon, in particular, has been called 'a significant and worrying escalation of the cyber threat that is expected to continue rising in future' [p.55, 117]. This attack has also been discussed specifically as 'an act of cyberwarfare' rather than as cybercrime or an otherwise uncategorized hacktivism that does not involve state competition [p.14, 118].

Nevertheless, the following case study demonstrates how, even under seemingly inflammatory geopolitical conditions, cyber warfare functions as a non-escalatory component of state competition. Despite clear tensions between rivals, cyber-to-kinetic escalation appears to be unattractive, meaning that state-sponsored or state-led malicious cyber activities remain below the threshold of war. While cyber warfare exists, there is no cyber security 'dilemma'.

What Happened During Shamoon?

At 11 am on 15 August 2012, the state-owned oil company Saudi Aramco suffered a huge loss of files to a self-replicating virus that was later referred to as Shamoon or DisTrack. In infected machines, the malware overwrote master boot records, making those computers inoperable and their data irretrievable [119]. Screens were then left displaying the corrupted and pixelated partial image of a burning American flag.

Although the nerve of attacking the world's largest oil producer led US Secretary of Defense Leon Panetta to label Shamoon as 'sophisticated', this was not an accurate description [p.62, 120]. Symantec identified three modules constituting the virus: a dropper that contained the original source of infection; a wiper that harvested and destroyed data; a reporter that was intended to deliver information back to the attacker [121]. Seculert described this as two-stage process of initial infection and use of that computer as a proxy for an external command-and-control server that spread the virus to other workstations before a relay mechanism was supposed to report back to the external server [122]. These mechanisms were not stealthy; they derived from a commercially available product called RawDisk, and the reporting stage also seemed to be ineffective [120]. This led Kaspersky to conclude that Shamoon suffered from 'some amateurish errors' [123].

Instead of technical prowess, the malware's success derived in no small measure from a strategic awareness of context-dependent human factors. It is likely that the original infection was delivered via spearphishing emails. The loss of data from infected machines has prevented a clear chain of evidence. Nevertheless, later related attacks have utilized 'recruitment-themed lures' with malicious links to otherwise genuine job descriptions on well-known employment sites that were tailored to specific employees [p.20, 124]. It is reasonable to consider that the original Shamoon malware was deployed using similarly astute tactics, including obtaining security credentials from some Aramco employees [p.14, 118]. The malware also included a logic bomb to time the attack during a national religious holiday when IT staff numbers at Saudi Aramco were particularly low [125].

As Shamoon represented a brazen attack on critical national infrastructure—in an already volatile region, which also appeared to have implications for energy markets worldwide—the incident sparked immediate fears of escalation towards war.

Did the Costs Demand Kinetic Retaliation?

There are two ways to categorize this attack: as a successful infiltration and disruption of Aramco's commercial activities with high financial, operational and reputational costs—or as a failed attempt to halt or disrupt oil production.

Initial reports masked the scale of the damage. Bronk and Tikk Ringas noted in 2013 that Saudi Aramco 'took almost two weeks to recover' [p.81, 119]. However, Pagliery approximates that it took 5 months for Aramco to return to normal operations, with a cost of $10 million to $100 million in damaged goods [125, 127]. The additional cost of recovery and capacity building—in the form of a genuine (competitively recruited, trained and managed) security and network operations centre (SNOC) and computer emergency response team (CERT) for home sites and regional offices—is then estimated at closer to half a billion dollars [125].

During recovery, the company had no immediate access to phones, no email for months and had to communicate via fax machines. As the Shamoon attack wiped Saudi Aramco's hard drives, they needed a huge new quantity to resurrect operations as quickly as possible. This led Aramco to use its fleet of private planes to collect hard drives directly from production floors in Southeast Asia, increasing the worldwide cost of hard drives in the process [125]. Payment systems also failed to function, leading to long queues of oil tankers waiting to be filled weeks after the attack, as well as legal contractual issues and a temporary fuel shortage within Saudi Arabia that carried unclear economic implications [126].

The human toll was also significant. Employees at Saudi Aramco had functioned as though 'part of a family', and so the Shamoon attack left a pervasive feeling of vulnerability as though their personal home had been violated [125]. Having witnessed this first-hand,

Kubecka notes that the psychological impact was serious enough to be labelled as something close to PTSD [125].[1]

The result was a demonstrable increase in everyday anxiety with physiological consequences and new implications for staff management. In November 2013, employees could not log onto their machines. Some panicked, taking pictures of their screens and posting them to Twitter to raise the alarm that they were under attack again—they were not. General distrust of IT systems also meant that even small and simple changes to minor systems required a multi-stage, 3-month procedure for approval [125]. The 'costs' associated with these types of setbacks are difficult to quantify.

Nevertheless, Saudi Aramco's industrial control systems (ICS) were isolated, and so the Shamon malware did not impact oil production. The company's vice president for corporate planning, Abdullah Al-Saada, called Shamoon a failure for this reason [120]. This is discussed among commentators as though leaving Aramco ICS in pristine condition was an oversight or mistake, leading to the fear that worse attacks and escalation would follow. This rather dismisses the possibility that Shamoon's creators possessed enough intelligence about the company to target specific employees with spearphishing techniques and inflict heavy costs but remain below a clear threshold for war.

Who Would be the Target of Any Retaliation?

The general consensus classifies Shamoon as an act of cyber warfare orchestrated by Iran [128]. Immediately after the attack, a new organization called The Cutting Sword of Justice, as well as a different anti-oppression hactivist group, both claimed responsibility for Shamoon [119]. These groups were largely dismissed as a front.

Instead, speculation focused on Saudi Arabia's most obvious geopolitical rival with a history of competitive interactions. Bronk and Tikk Ringas refer to this as 'a reasonable inference' (2013, 88). After the discovery of Stuxnet, Iran had reportedly invested more than a billion dollars in developing its cyber capabilities [129]. The wiper code within Shamoon was also similar to the Flame virus discovered within Iran's Ministry of Energy. In addition, Bronk and Tikk Ringas note that 'It is implausible that the Iranian government, which monitors the country's Internet for political purposes, was not aware of a major cyber operation consuming significant bandwidth and originating from an internal source' [p.88, 119].

Subsequent events have tended to affirm rather than undermine the subjective credibility attribution of 2012. In 2017, FireEye called attention to a cyberattack group that they referred to APT33. Their report indicated that APT33 had been active since at least 2013 and was working on behalf of the Iranian government to conduct espionage within the military and commercial aviation sectors in the USA, Saudi Arabia and South Korea, as well as companies linked to energy production [130]. Using spearphishing emails to target company employees, APT33 was noted to possess destructive capabilities linked to the Shamoon malware, with the expectation that tools were being shared between Iranian-orchestrated groups [124].

By 2019, after several waves of these related wiper attacks, the fluid association of relevant Iran-backed actors had collectively been labelled as the 'Shamoon Group…also known as the Cutting Sword of Justice' [p.11, 116]. This refers to a somewhat amorphous entity rather than an ordered organization or hierarchy [131].

1 Kubecka recounts meeting one high ranking official whose hair had turned from black to white during the company's response to Shamoon (2015).

Did the Attack Itself Represent Novel Risks of Escalation?

When discussing motives for an Iran-orchestrated attack on Saudi CNI, existing scholarship tends to highlight one clear provocation rather than acknowledge the overall context of competitive interactions between geopolitical adversaries. This compartmentalized conception of Middle East conflict makes escalation from cyber to kinetic warfare, seen as a series of single acts and retaliations, seem possible and even likely. However, this not a useful abstraction. In practice, incidents reflecting the implicit rivalry between Saudi Arabia and Iran represent almost constant noise, in which cyber operations are just one component. This makes it nearly impossible to identify a specific act worthy of kinetic retaliation.

The tendency to highlight only one potential incitement is unhelpful. Shamoon is often blamed on the fact that Iran remained under internationally imposed sanctions in 2012 while Saudi Arabia was able to continue profiting from its oil resources [119, 120]. The Shamoon attack has also been explained as a retaliation for Stuxnet [127, 132]. Although these events might represent push factors that prompted Iran to develop its cyber capabilities, highlighting a single cause somewhat glosses over multifaceted Gulf state interactions.

Rather than any single provocation, it is possible to identify complex interactions effects related to the Arab Spring, Saudi intervention in Bahrain, P5 + 1 negotiations and the Syrian civil war. This demonstrates how there was and remains constant, complex and indirect practices of rivalry between Iran and its neighbours, in which Shamoon makes sense only as a continuation of deliberately limited warfare.

Both Saudi Arabia and Iran had faced internal waves of protest in 2011 and 2012 related to grievances associated with the Arab Spring. Both regimes were sensitive to dissent, feared the other's influence on sectarian divisions, used draconian measures to quell their protest movements and issued statements blaming foreign enemies for fomenting the unrest [133, 134]. Neither Saudi nor Iranian decision-makers chose to blame each other directly.

Indeed, Saudi–Iranian political interactions during this time represented opposing stances on almost every issue but maintained a veneer of diplomatic civility. In March 2011, Bahrain requested Saudi troops to help protect the government from a Shi'a majority demanding greater political representation. In response to this Saudi intervention, the usually bombastic Iranian president, Mahmoud Ahmadinejad, refrained from condemning it and merely called for a 'fair and Islamic solution' [135].

By August 2012, Iran's nuclear negotiations with the P5 + 1 had also been progressing and stalling for over 3 years. During this time, Iran repeatedly defied enrichment restrictions and lashed out against the perceived unfairness of sanctions. A total of 2 weeks after the Shamoon attack on Saudi Aramco, the International Atomic Energy Agency (IAEA) reported that Iran had increased the number of centrifuges installed at its Fordow enrichment plant and was continuing to enrich uranium beyond its needs [136]. This kind of figurative flexing on the world stage had become routine.

Additionally, such attempted power projections were almost certainly viewed within Iran as necessary to offset the Saudi–Emirati–Western challenge to its only regional ally (Syria's Assad regime), while also having to face an Islamic State threat that was partially funded by or through its local rivals. Nevertheless, despite being 'at each other's throats' in these foreign policy spheres, public interactions remained restrained [137]. President Ahmadinejad was invited to Saudi Arabia immediately after the Shamoon attack in August

2012 to participate in a conference of the Organization of Islamic Cooperation—and any wars of words were delegated to lower ranking officials [137].

With these subtle and indirect real-world interactions in mind, it becomes unrealistic to conceptualize the existence of a cyber security dilemma, which requires that cyberattacks be viewed as single events outside of the normal pattern of indirect rivalry.

How did Saudi Arabia Respond?

It is important to recognize that Saudi Arabian authorities treated Shamoon as an internal problem, despite the near certainty that it was an Iranian orchestrated attack [138]. This reflects two expectations discussed above. The traditional systemic analysis indicates that cyberattacks are unlikely to generate a new arms race in which heightened tension and the miscalculation of retaliatory risks escalates directly to kinetic warfare. When introducing psychological variables into this analysis (material contexts, societal contexts and personal cognition) again the expectation is that, if the adversaries are not already openly at war, then state leaders should be more inclined to minimize and deescalate after cyberattacks than escalate to kinetic responses. The exception would be if a target state interpreted cyber warfare as an attack on its own leader's political survival, but there are no instances of this occurring at the time of writing.

In 2012, before the attack occurred, Saudi Brigadier General, Prince Naef Bin Ahmed Al-Saud acknowledged that a cyberattack on Saudi Aramco 'could be considered a national security threat'; after the attack occurred, he referred to it as an assault on 'the Kingdom's economy as a whole' [p.74, 129]. This rhetoric mirrored the standard posturing associated with threat-based deterrence, which aims to avoid the steady erosion of credibility that might embolden an adversary. As noted above, this type of deliberately hyperbolic rhetoric is a core component of American cyber deterrence. It is intended to increase any potential attacker's perception of the inherent risks in using cyberattacks against the relevant target state (but also seems generate fear among observers who interpret implicit threats as inherently inflammatory).

Therefore, it is crucial to note that, despite the uncompromising public posturing beforehand, Saudi Arabia's Ministry of Foreign Affairs never became directly involved in the response to Shamoon. The Kingdom swallowed and absorbed this attack rather than directly escalating the situation (militarily or diplomatically) in response. Other than Aramco itself, it was Saudi Arabia's Ministry of Interior that offered governmental support and comment, even confirming that the attack originated from several countries that the spokesman declined to name [p.3–4, 138]. The Ministry of the Interior also handled investigations into Shamoon's origin and costs. The official results have never been published, and, despite widespread discussion regarding the role of Iran, neither Saudi Aramco nor the government have chosen to name the suspected perpetrator [p.3–4, 138]. This low-key response was entirely in keeping with established practices of Gulf state rivalry, again highlighting how cyber warfare occurs within the pre-existing patterns of securitized relationships in a way that is almost reassuringly familiar.

It was also predictable that the Kingdom would seek to downplay Shamoon's damaging effects, to maintain confidence in Aramco worldwide and to deny Iran that strategic objective. As noted above, a minimizing strategy is attractive because the material risks are very low compared to escalation, and there appears to be a general feeling across multiple societies that escalation from cyber to kinetic warfare is neither valid nor acceptable. Instead of lashing out, Saudi Arabia focused on developing deterrence through denial. Subsequent growth in the Saudi cybersecurity sector also complemented the ruling family's desire to suppress internal dissent and target dissidents abroad [139]. In 2013, Saudi Arabia adopted its first National Cybersecurity Strategy and, in 2017, unveiled its National Cyber Security Center at the Ministry of the Interior. The Kingdom was then successful in lobbying the USA to aid in continuing the modernization of its cybersecurity apparatus as part of a deal worth $110 billion [140, 141].

Despite the atmosphere of high tension, as well as both Iran and Saudi Arabia's previous willingness to engage in kinetic warfare in proxy situations, escalation specifically from cyber to kinetic attacks did not occur between them. Indeed, as there are no existing cases of escalation from cyber to traditional warfare between states at the time of writing, this case is illustrative rather than determinative. It does provide a real-world example that should assuage some of the observer fears noted above, but a slightly longer-term assessment is needed to address whether the risk of escalation between Saudi Arabia and Iran increased after this attack. This is discussed briefly below.

Has the Risk of Escalation Increased?

To argue that Shamoon did not represent or initiate a new arms race or spiral associated with traditional security dilemma, it is vital to recognize that cyber warfare has become normal in the Gulf. The use of cyberattacks to achieve limited objectives has become the status quo between Iran and its rivals. The Qatari firm RasGas suffered a very similar Shamoon attack only 2 weeks after the initial assault on Aramco systems. Another version of Shamoon targeted thousands of Saudi government, civil aviation and private firm computers in November 2016 and January 2017, with infected machines left displaying an image of the drowned Syrian child, Aylan Kurdi—presumably as an indictment of regional support for rebel groups in the Syrian civil war. This Shamoon 2.0 also spread within other Gulf state organizations [124].

Again, these attacks have often been discussed out of their full context, with Crowdstrike raising the possibility that Iran could be retaliating for American reinstatement of sanctions [p.17, 116]. However, interpreting Iran's multiple and frequent cyberattacks on its neighbours as responses to specific American activities (rather than part of long-standing political dynamics in the Gulf) is a red herring. Incidents of American actions against Iran are too sparse to be seen as the primary driver behind Iran's frequent cyberattacks against its close neighbours and further afield. Focusing on the USA versus Iran relationship may also be fuelling unnecessary fears of cyber-to-kinetic escalation simply because of the emotionally charged nature of American discourse on the perceived Iranian threat. The observable reality is that cyber warfare has been absorbed into the cannon of regional Gulf interactions. As well as avoiding escalation from cyber to kinetic attacks, Saudi Arabia seems to have demurred from retaliations within cyberspace. Shamoon resurfaced again in 2018 and January 2019, validating the growth of Saudi Arabian cybersecurity organizations as well as American investment in this sector. Crucially, at the time of writing, Saudi Arabia is not associated with any state-led cyberattacks on its geopolitical rivals.

As Connell noted of cyber warfare in 2014, 'the genie is now 'out of the bottle'' [p.7 142]. However, there appears little evidence in support of the catastrophic thinking associated with a traditional security dilemma. Kaush warns of 'overtly aggressive operations that

cross a red line' but neglects to appreciate that rivals regularly engage in aggressive actions while purposely remaining below the threshold that would warrant kinetic responses [p.7, 115]. Instead, the response to these cyberattacks has been a focus on internal balancing, domestic control and generating deterrence by denial.

Conclusion

Although the fear of escalation from cyber to kinetic warfare is understandable, a multi-level NCR perspective provides overlapping but reassuring theory-based insights that are reflected in an illustrative narrative of the Shamoon attack in 2012. Cyber capabilities cannot be measured separately and so cannot alter the distribution of power, meaning it is not possible for states to attempt the kind of balancing associated with incendiary arms races. A classical realist assessment indicates that cyber warfare is an attractive mechanism specifically because it operates outside of the escalatory spiral.

Adding an awareness of sub-state psychological variables to generate the NCR assessment also provides cause for calm. The incomplete material conditions associated with cyber warfare make escalation cognitively unattractive, and societal cues limit the complexity of cyber warfare while ontologically rejecting escalation. Additionally, pre-existing security relationships define adversaries in cyberspace, meaning that military planners do not have to fathom a vast domain of threats—the new enemies are the same as the old ones. Instead of an arms race, what we are witnessing is a contest between state bureaucracies over who can channel the most expertize and resources, as well as public- and private-sector cooperation, into patching vulnerabilities, removing legacy systems and developing better attribution and cyber hygiene mechanisms. When reduced to these activities, state competition in cyberspace seems decidedly less inflammatory.

Importantly, key events of the original Shamoon attack and Saudi Arabia's response to this instance of cyber warfare illustrate how a multi-level Neoclassical reasoning against the existence of a cyber security dilemma functions in practice. Not all elements of the structural assessment, and not every psychological variable, will be equally relevant in every case, but the conceptual argument presented in this paper demonstrates multiple overlapping routes to the same conclusion—that there is no new cyber arms race and no specifically cyber security dilemma.

Although there is some disagreement about whether NCR is capable of more than this midrange theory approach—see for example, [49]—this paper asserts that escalation in cyber warfare is so multi-faceted as a problem that it would be highly unwise to ignore the piecemeal, midrange theoretical approaches facilitated by NCR [40]. One area of concern would be the use of cyber capabilities to target a foreign regime's political survival. Such operations seem low-risk because the expected effects are non-destructive, but the threat could be perceived as politically existential. This might provide an inadvertent route to escalation of which policymakers should be wary. Thus, an NCR perspective also highlights more and different topics deserving of attention as we attempt to understand the ramifications of mutually assured disruption (if not destruction) as well as the mechanisms and consequences of purposeful information warfare.

Therefore, the arguments presented above indicate that future analysts and strategists should, as a minimum requirement, consider two questions when seeking to identify any dangers of escalation from cyber to kinetic warfare in response to real world events: Does the situation alter the balance of power? Does the situation threaten any leader's political survival?

Acknowledgements

The author would like to thank Professor Julian Williams and attendees of the Durham-Dartmouth Global Hub for their useful insights, as well as the journal editors and reviewers for their helpful suggestions and comments.

Competing Interest

There is no competing interest.

References

1. Layne C. The war on terrorism and the balance of power: the paradoxes of American hegemony. In: Paul T.V., Wirtz J J., Fortmann M, (eds.), *Balance of Power: Theory and Practice in the 21st Century*. Stanford: Stanford University Press, 2004.
2. Jervis R. *Perception and Misperception in International Politics: New Edition*. Princeton: Princeton University Press, 2017.
3. Glaser CL. The security dilemma revisited. *World Polit* 1997;**50**:171–201.
4. Buchanan B. *The Cyber Security Dilemma: Hacking, Trust, and Fear Between Nations*. New York: Oxford University Press, 2017.
5. Pomerleau M. *Why More Research is Needed to Craft Good Cyber Policy*. Washington: Fifth Domain, 2020. February 13. https://www.fifthdomain.com/thought-leadership/2020/02/13/why-more-research-is-needed-to-craft-good-cyber-policy/. (30 June 2022, date last accessed).
6. Jensen B, Valeriano B. 'What do we know about cyber escalation? observations from simulations and surveys,' Scowcroft Centre for Strategy and Security, Washington: Atlantic Council. Issue Brief. 2019. November. https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf. (30 June 2022, date last accessed).
7. Rid T. *Cyber War Will Not Take Place*. London: C. Hurst & Co, 2013.
8. Liff AP. The proliferation of cyberwarfare capabilities and interstate war, redux: Liff responds to Junio. *J Strateg Stud* 2013;**36**:134–8.
9. Singer PW, Friedman A. *Cybersecurity and Cyberwar: What Everyone Needs to Know* Oxford: Oxford University Press, 2014.
10. Borghard ED, Lonergan SW. Cyber operations as imperfect tools of escalation. *Strateg Stud Quart* 2019;**13**:122–45.
11. Schneider J. Cyber and crisis escalation: insights from wargaming. USASOC Futures Forum. Fort Bragg: USASOC. 2017. https://pacs.einaudi.cornell.edu/sites/pacs/files/Schneider.Cyber%20and%20Crisis%20Escalation%20Insights%20from%20Wargaming%20Schneider%20for%20Cornell.10-12-17.pdf. (30 June 2022, date last accessed).
12. Morgan PM. Applicability of traditional deterrence concepts and theory to the cyber realm. In: *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: National Academies Press, 2010.
13. Shalal-Esa A. Ex-U.S. general urges frank talk on cyber weapons. London: Reuters. 2011. November 5. https://www.reuters.com/article/us-cyber-cartwright-idUSTRE7A514C20111106. (30 June 2022, date last accessed).
14. Singer PW. How the United States can win the cyberwar of the future. Washington: Foreign Policy. 2015. December 18. https://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/. (30 June 2022, date last accessed).
15. Starks T. Trump talks 'the cyber'. Arlingto: Politico. 2020. January 13. https://www.politico.com/newsletters/morning-cybersecurity/2020/01/13/trump-talks-the-cyber-784328. (30 June 2022, date last accessed).
16. Wilke C. Joe Biden warns he will be tough on state sponsors of cyberattacks, as U.S. suffers massive hack. CNBC. 2020. December 20. https://www.cnbc.com/2020/12/17/biden-hints-at-a-tougher-stance-against-state-sponsors-of-cyberattacks.html. (30 June 2022, date last accessed).

17. Kreps S, Schneider J. Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. *J Cybersecur* 2019;**5**:1–11.
18. Department of Defense. Nuclear Posture Review. 2018. https://dod.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx. (30 June 2022, date last accessed).
19. United States of American Cyberspace Solarium Commission. 2020. https://www.solarium.gov. (30 June 2022, date last accessed).
20. Lupovici A. Cyberwarfare and deterrence: trends and challenges in research. *Milit Strat Aff* 2011;**3**:49–61.
21. Glaser C. *Deterrence of Cyberattacks and US National Security*. Cyber Security Policy and Research Institute Report GW-CSPRI-2011-5. Washington: The George Washington University, 2011.
22. Betz D, Stevens T. *Cyberspace and the State: Toward a Strategy for Cyber Power*. Oxon: Routledge, 2011.
23. Saltzman I. Cyber posturing and the offense-defense balance, *Contemp Secur Policy* 2013;**34**:40–63.
24. Clarke RA, Knake RK. *Cyber War*. Old Saybrook: Tantor Media Inc, 2014.
25. Mandel R. *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*. Washington: Georgetown University Press, 2017.
26. Slayton R. What is the cyber offense-defense balance? Conceptions, causes, and assessment. *Int Secur* 2017;**41**:72–109.
27. Olejnik L. Global consequences of escalating US-Russia cyber relations. Council on Foreign Relations. 2019. April 2. https://www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict. (30 June 2022, date last accessed).
28. Lindsay N. The Rise of the Global Cyber War Threat. CPO Magazine. 2019. August 5. https://www.cpomagazine.com/cyber-security/the-rise-of-the-global-cyber-war-threat/. (30 June 2022, date last accessed).
29. Andriole S. Cyber warfare will explode in 2020 (because it's cheap, easy and effective. Jersey City: Forbes. 2020. January 14. https://www.forbes.com/sites/steveandriole/2020/01/14/cyberwarfare-will-explode-in-2020-because-its-cheap-easy---effective/. (30 June 2022, date last accessed).
30. Acton JM. Cyber warfare and inadvertent escalation. *Daedalus* 2020;**149**:133–49. March 25. https://carnegieendowment.org/2020/03/25/cyber-warfare-and-inadvertent-escalation-pub-81377. (30 June 2022, date last accessed).
31. Klare MT. Cyber battles, nuclear outcomes? Dangerous new pathways to escalation. Arms Control Association. 2019. https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation. (30 June 2022, date last accessed).
32. Maurer T. The future of war: cyber is expanding the clausewitzian spectrum of conflict. Foreign Policy. 2014. November 13. https://foreignpolicy.com/2014/11/13/the-future-of-war-cyber-is-expanding-the-clausewitzian-spectrum-of-conflict/. (30 June 2022, date last accessed).
33. Hurwitz R. Keeping cool: steps for avoiding conflict and escalation in cyberspace. *Georget J Int Aff* 2013:17–28.
34. Lin H. Escalation dynamics and conflict termination in cyberspace. *Strateg Stud Quart* 2012;**6**:46–70.
35. Deibert RJ. Bounding cyber power: escalation and restraint in global cyberspace. In: *Organized Chaos: Reimagining the Internet*. Waterloo: CIGI, 2014.
36. Cavaiola LJ, Gompert DC, Libicki M. Cyber house rules: on war, retaliation and escalation. *Survival* 2015;**57**:81–104.
37. Kostyuk N, Powell S, Skach M. Determinants of the cyber escalation ladder. *Cyber Def Rev* 2018;**3**:123–34.
38. Perlroth N. *This Is How They Tell Me the World Ends: The Cyber Weapons Arms Race*. London: Bloomsbury, 2021.
39. Healey J, Jenkins N. Rough-and-ready: a policy framework to determine if cyber deterrence is working or failing. In: *Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon)*. Tallinn: Cooperative Cyber Defence Centre of Excellence, 1–20, 2019.
40. Libicki MC. *Crisis and Escalation in Cyberspace*. Santa Monica: Rand Corporation, 2012.
41. Jasper S. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. New York: Rowman & Littlefield, 2017.
42. Whyte C, Mazanec B. *Understanding Cyber Warfare: Politics, Policy and Strategy*. Oxon: Routledge, 2018.
43. Valeriano B, Jensen BM, Maness RC. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press, 2018.
44. Junio TJ. How probable is cyber war? Bringing IR Theory back into the cyber conflict debate. *J Strateg Stud*. 2013;**36**:125–33.
45. Farrell H, Glaser CL. The role of effects, saliencies and norms in US cyberwar doctrine. *J Cybersecur* 2017;**3**:7–17.
46. Jervis R. Some thoughts on deterrence in the cyber era. *J Inf Warf* 2016;**15**:66–73.
47. Clausewitz C. Howard M, Paret P. *On War*. Translated by. Princeton: Princeton University Press, 1976.
48. Hudson V. *Foreign Policy Analysis: Classica and Contemporary Theory*. London: Rowman & Littlefield, 2006.
49. Meibauer G, Desmaele L, Onea T. *et al*. Forum: rethinking neoclassical realism at theory's end. *Int Stud Rev* 2020;**23**:268. doi: 10.1093/isr/viaa018.
50. Rathbun B. A rose by any other name: neoclassical realism as the logical and necessary extension of structural realism. *Secur Stud* 2008;**17**:294–321.
51. Götz E. Enemy at the gates: a neoclassical realist explanation of Russia's baltic policy. *Foreign Pol Anal* 2019;**15.1**:99–117.
52. Labs E. Beyond victory: offensive realism and the expansion of war aims. *Secur Stud* 1997;**6**:1–49.
53. Yordan CL. America's quest for global hegemony: offensive realism, the bush doctrine, and the 2003 Iraq war. *Theor J Soc Polit Theory* 2006;**110**:125–57.
54. Schmidt BC. Competing realist conceptions of power. *Millenn J Int Stud* 2005;**33**:523–49.
55. Toft P. John J. Mearsheimer: an offensive realist between geopolitics and power. *J Int Relat Dev* 2005;**8**:381–408.
56. Lobell SE, Ripsman NM, Taliaferro JW. *Neoclassical Realism, the State, and Foreign Policy*. Cambridge: Cambridge University Press, 2014.
57. Nygren B. Using the neo-classical realism paradigm to predict Russian foreign policy behaviour as a complement to using resources. *Int Polit* 2012;**49**:517–29.
58. Waltz K. Realist thought and neorealist theory. In: *The Evolution of Theory in International Relations*. Rothstein R (ed.), South Carolina: University of South Carolina Press, 1992, 21–38.
59. Kirshner J. The tragedy of offensive realism: classical realism and the rise of China. *Eur J Int Relat* 2012;**18**:53–75.
60. Mearsheimer JJ. *The Tragedy of Great Power Politics*. New York: WW Norton & Company, 2001.
61. Nye JS, Jr. Get smart: combining hard and soft power. *Foreign Aff* 2009;**88**:160–3.
62. Walt SM. Alliance formation and the balance of world power. *Int Secur* 1985;**9**:3–43.
63. Pashakhanlou AH. *Realism and Fear in International Relations*. Cham: Palgrave Macmillan, 2017.
64. Paul TV. Introduction: the enduring axioms of balance of power theory and their contemporary relevance. In: Paul T.V., Wirtz J J, Fortmann M (eds.), *Balance of Power: Theory and Practice in the 21st Century*. Stanford: Stanford University Press, 2004.
65. Nye J. Introduction. In: Rotberg RI., Theodore KR (eds.), *The Origin and Prevention of Major Wars*. Cambridge: Cambridge University Press, 1989.
66. Bennett C. John Bolton, Cyber Warrior. Politico. 2018. April 1. https://www.politico.eu/article/john-bolton-us-national-security-adviser-cyber-digital-warfare-cyberspace-warrior/. (30 June 2022, date last accessed).
67. Rose G. Neoclassical realism and theories of foreign policy. *World Polit* 1998;**51**:144–72.

68. Levy J. Psychology and foreign policy decision-making. In: Huddy L., Sears D., Levy J. (eds.), *Oxford Handbook of Political Psychology*. 2nd edn. Oxford: Oxford University Press, 2013, 301–33.
69. Ellman C. Horses for courses: why nor neorealist theories of foreign policy? *Secur Stud* 1996;**6**:7–53.
70. Smith N. Can neoclassical realism become a genuine theory of international relations? *J Polit* 2018;**80**:742–9.
71. The International Institute for Strategic Studies (IISS). Cyber capabilities and national power: a net assessment. London: IISS. 2021.
72. Guardian T. Russia denies disrupting GPS signals during NATO arctic exercises. The Guardian. 2018. November 12. https://www.theguardian.com/world/2018/nov/12/russia-denies-blame-for-arctic-gps-interference. (30 June 2022, date last accessed).
73. Crerar P, Henley J, Wintour P. Russia accused of cyberattack on chemical weapons watchdog. The Guardian. 2018. October 4. https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body. (30 June 2022, date last accessed).
74. Fearon JD. Signaling versus the balance of power and interests: an empirical test of a crisis bargaining model. *J Confl Resolut* 1994;**38**:236–69.
75. Hutchins EM, Cloppert MJ, Amin RM. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Bethesda: Lockheed Martin Corporation, 2011, 4–5.
76. Gartzke E, Lindsay JR. Weaving tangled webs: offense, defense, and deception in cyberspace. *Secur Stud* 2015;**24**:316–48.
77. *United States Cyber Command*. Statement of General Paul M. Nakasone, Commander, United States Cyber Command Before the Senate Committee on Armed Services. 2019. February 14. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf. (30 June 2022, date last accessed).
78. Carroll O. US cyber attack: did American really try to override the russian power grid?. Independent. 2019. June 19. https://www.independent.co.uk/news/world/europe/us-cyber-attack-russia-power-grid-war-kremlin-a8964506.html. (30 June 2022, date last accessed).
79. Al-Mulhim RA, Al-Zamil LA, Al-Dossary FM. Cyber attacks on Saudi Arabia environment. *Int J Comput Netw Commun Secur* 2020;**8**:26–31.
80. Caspit B Israel's response to cyber attack sends clear warning to Iran. Al Monitor. 2020. May 22. https://www.al-monitor.com/pulse/originals/2020/05/israel-us-iran-mike-pompeo-aviv-kochavi-cyberattack-port.html. (30 June 2022, date last accessed).
81. Paul K. What you need to know about the biggest hack of the US Government in years. The Guardian. 2020. https://www.theguardian.com/technology/2020/dec/15/orion-hack-solarwinds-explained-us-treasury-commerce-department. (30 June 2022, date last accessed).
82. Kydd A. Game theory and the spiral model. *World Polit* 1997;**49**:371–400.
83. Borghard ED, Lonergan SW. Deterrence by denial in cyberspace. *J Strateg Stud* 2021;**4**:1–36
84. Nye JS. Deterrence and dissuasion in cyberspace. *Int Secur* 2016;**41**:44–71.
85. Subramanian VS. Talk given at the Durham-Dartmouth Global Debate on Cybersecurity in December 2019. Washington: Durham University News, 2019.
86. Groll E. Trump and his lieutenants are cyber hawks. Will they play hardball with Putin?. Foreign Policy. 2016. December 16. http://foreignpolicy.com/2016/12/16/trump-and-his-lieutenants-are-cyber-hawks-will-they-play-hardball-with-putin/#. (30 June 2022, date last accessed).
87. Gross Stein J. Threat perception in International Relations. In: Huddy L., Sears D. O., Levy J. (eds.), *The Oxford Handbook of Political Psychology*, Oxford: Oxford University Press, 2013, 364–94.
88. Gries P, Sanders M. Whom do we trust? Testing for socialization effects in chinese surveys. In: Johnston A. I., Shen M. (eds.), *Perception and Misperception in American and Chinese Views of the Other*, Washington, DC: Carnegie Endowment for International Peace, 2015, 41–62.
89. Sinkkonen E, Elovainio M. Chinese perceptions of threats from the United States and Japan. *Polit Psychol* 2020;**41**:265–82.
90. Schaub G, Jr. Deterrence, compellence, and prospect theory. *Polit Psychol* 2004;**25**:389–411.
91. Rose McD, Cowden J, Koopman C. Framing, uncertainty, and hostile communications in a crisis experiment. *Polit Psychol* 2002;**23**:133–49.
92. Geva N, Hanson DC. Cultural similarity, foreign policy actions, and regime perception: an experimental study of international cues and democratic peace. *Polit Psychol* 1999;**20**:803–27.
93. Garcia-Retamero R, Müller SM, Rousseau DL. The impact of value similarity and power on the perception of threat. *Polit Psychol* 2012;**33**:179–93.
94. Buzan B. *People, States, and Fear: The National Security Problem in International Relations*. Sussex: Wheatsheaf Books, 1983.
95. Wendt A. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999.
96. Gries P, Zhang Q, Michael Crowson H, Cai H. Patriotism, nationalism and china's us policy: structures and consequences of chinese national identity. *Chin Quart* 2011;**205**:1–17.
97. Braw E. Forget Washington and Beijing. These days global leadership comes from Berlin. Foreign Policy. 2020. April 28. https://foreignpolicy.com/2020/04/28/global-leadership-coronavirus-pandemic-germany-united-states-china/. (30 June 2022, date last accessed).
98. Gaston S. Public opinion on global threats and the future of NATO. British Foreign Policy Group. 2019. December 3. https://bfpg.co.uk/2019/12/public-opinion-on-global-threats-future-of-nato/. (30 June 2022, date last accessed).
99. Chaturvedi A. Map shows which countries are the biggest threats to peace. Geo-Spatial World. 2018. January 4. https://www.geospatialworld.net/blogs/countries-biggest-threat-to-peace/. (30 June 2022, date last accessed).
100. Yarhi-Milo K. *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations*. Princeton: Princeton University Press, 2014.
101. Zetter K. How digital detectives deciphered stuxnet, the most menacing malware in history. Wired. 2011. July 11. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/. (30 June 2022, date last accessed).
102. Keller J, Yang YiE. Problem representation, option generation, and poliheuristic theory: an experimental analysis. *Polit Psychol* 2016;**37**:739–52.
103. Sprout HH, Sprout M. *Ecological Perspective on Human Affairs*, Princeton: Princeton University Press, 1965.
104. Golec A. Cognitive skills as predictor of attitudes toward political conflict: a study of polish politicians. *Polit Psychol* 2002;**23**:731–57.
105. Keys B, Yorke C. Personal and political emotions in the mind of the diplomat. *Polit Psychol* 2019;**40**:1235–49.
106. Mintz A, Geva N, (eds.), *Decisionmaking on War and Peace: The Cognitive-Rational Debate*. New York: Lynne Rienner Publishers, 1997.
107. DeRouen K, Jr., Sprecher C. Initial crisis reaction and poliheuristic theory. *J Confl Resolut* 2004;**48**:56–68.
108. Beckerman C. *Unexpected State: British Politics and the Creation of Israel*. Bloomington: Indiana University Press, 2020.
109. Brown J, Fazal T. #SorryNotSorry: why states neither confirm nor deny responsibility for cyber operations. *Eur J Int Secur* 2021;**6**:401–17.
110. Astorino-Courtois A, Trusty B. Degrees of difficulty: the effect of Israeli policy shifts on syrian peace decisions. In: *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making*. Mintz A (ed.), New York: Palgrave Macmillan, 2002, 29–54.
111. Sandywell B. Monsters in cyberspace cyberphobia and cultural panic in the information age. *Inf Commun Soc* 2006;**9**:39–61.
112. Whyte C. Beyond tit-for-tat in cyberspace: political warfare and lateral sources of escalation online. *Eur J Int Secur* 2020;**5**:195–214.

113. Post J. *Narcissism and Politics: Dreams of Glory*. Cambridge: Cambridge University Press, 2014.
114. Committee on Armed Services House of Representatives. *111th Congress, 2nd Session, U.S. Cyber Command: Organizing for Cyberspace Operations*. Government Publishing Office, 2010. September 23. https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg62397/pdf/CHRG-111hhrg62397.pdf. (30 June 2022, date last accessed).
115. Kausch K. How cyber geopolitics will destabilize the Middle East. Policy Brief. Washington: German Marshall Fund of the United States. 2017.
116. Bazner M. *Iranian Cyber Activities in the Context of Regional Rivalries and International Tensions*. Zurich: Center for Security Studies (CSS), 2019.
117. Onyeji I, Bazilian M, Bronk C. Cyber security and critical energy infrastructure. *Electr J* 2014;**27**:52–60.
118. Tolga IB. *Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2018.
119. Bronk CT, Ringas E. The cyber attack on Saudi Aramco. *Survival* 2013;**55**:81–96.
120. Guitton C, Korzak E. The sophistication criterion for attribution. *RUSI J* 2013;**158**:62–8.
121. Symantec. The Shamoon attacks. Symantec Blog. 2012. 16 August. Cited in (Bronk and Tikk Rinus 2013). http://www.symantec. com/connect/blogs/shamoon-attacks. (30 June 2022, date last accessed).
122. Seculert. Shamoon, a two-stage targeted attack. Seculert Blog. 2012. 16 August. Cited in (Bronk and Tikk Rinus 2013. http://blog.seculert.com/2012/08/shamoon-two-stage-targeted-attack.html. (30 June 2022, date last accessed).
123. Tarakanov D. Shamoon the wiper: further details (Part II). SecureList. 2012. 11 September. https://securelist.com/shamoon-the-wiper-further-details-part-ii/57784/.
124. Hemsley K, Fisher R. *History of Industrial Control System Cyber Incidents*. Idaho Falls: Idaho National Laboratory, US Department of Energy, Office of Nuclear Energy, 2018.
125. Kubecka C. *How to Implement IT Security After a Cyber Meltdown*. Black Hat Official YouTube Channel, 2015. https://www.youtube.com/watch?v=WyMobr_TDSI. (30 June 2022, date last accessed).
126. Pagliery J. The inside story of the biggest hack in history. CNN. 2015. 5 August. https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html. (30 June 2022, date last accessed).
127. Anderson C, Sadjadpour K. *Iran's Cyber Threat Espionage, Sabotage and Revenge*. Washington: Carnegie Endowment for International Peace, 2018.
128. Work JD. In wolf's clothing: complications of threat emulation in contemporary cyber intelligence PracticeIn: *Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. Oxford: IEEE. 2019, 1–8.
129. Zakariya D, Abokhodair N. Saudi Arabi'a Response to Cyber Conflict: A Case Study of the Shamoon Malware Incident. In: *Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics*. Seattle: IEEE, 2013, 73–5.
130. O'Leary J, Kimble J, Vanderlee K, Fraser N. Insights into Iranian cyber espionage: APT33 targets aerospace and energy sectors and has ties to destructive malware. FireEye. 2017. 20 September 2017. https://www.mandiant.com/resources/apt33-insights-into-iranian-cyber-espionage. (30 June 2022, date last accessed).
131. Ackerman G, Cole R, Thompson A, Orleans A, Carr N. OVERRULED: containing a potentially destructive adversary. FireEye. 2018. https://www.mandiant.com/resources/overruled-containing-a-potentially-destructive-adversary. (30 June 2022, date last accessed).
132. Bellovin S, Landau S, Lin H. Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *J Cybersecur* 2017;**3**:59–68.
133. BBC News. *Iran Protests Going Nowhere Says Mahmoud Ahmadinejad*. BBC News, 2011. 15 February. https://www.bbc.co.uk/news/world-middle-east-12475824. (30 June 2022, date last accessed).
134. Wehrey F. *The forgotten uprising in Eastern Saudi Arabia*. Carnegie Endowment for International Peace, 2013. 14 June. https://carnegieendowment.org/2013/06/14/forgotten-uprising-in-eastern-saudi-arabia-pub-52093. (30 June 2022, date last accessed).
135. Wigglesworth R. Ahmadi-Nejad condemns foreign troops in Bahrain. FT. 2011. 16 March. https://www.ft.com/content/5754805a-4e44-11e0-a9fa-00144feab49a. (30 June 2022, date last accessed).
136. Arms Control Association. *Timeline of Nuclear Diplomacy with Iran*. Arms Control Association, 2022. https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran#2012. (30 June 2022, date last accessed).
137. Miller E. For Saudi Arabia, despite Ahmadinejad's visit, Iran remains the snake. Times of Israel. 2012. 21 August. https://www.timesofisrael.com/for-saudi-arabia-depite-ahmadinejads-visit-iran-remains-the-snake/. (30 June 2022, date last accessed).
138. Van Der Meer S. *Foreign Policy Responses to International Cyber-Attacks: Some Lessons Learned*. The Hague: Clingendael Institute, 2015.
139. Ouassini A, Boynton K. The silicon valley of the Middle East: cybersecurity, Saudi Arabia, and the path to vision 2030. In: Romaniuk S, Manjikan M, (eds.), *Routledge Companion to Global Cyber-Security Strategy*. Oxon: Routledge, 2021.
140. Phelps J, Stuyk R. Trump signs $110 billion arms deal with Saudi Arabia on 'a tremendous day'. ABC News. 2017. 20 May. https://abcnews.go.com/Politics/trump-signs-110-billion-armsdeal-saudi-arabia/story?id=47531180. (30 June 2022, date last accessed).
141. Al Sharif DT. How Saudis are Protected against Cybercrime. Arab News. 2018. 11 April. www.arabnews.com/node/1282571. (30 June 2022, date last accessed).
142. Connell M. *Deterring Iran's Use of Offensive Cyber: A Case Study*. Washington: CNA Analysis & Solutions, 2014.