Military Operations in Cyberspace

Aaron Brantly and Max Smeets

Contents

Abstract

Over the years, experts – both in and outside of the military – have repeatedly stated that we need to improve our conceptual and doctrinal thinking when it comes to military cyber operations and how to address the cyber threat. The purpose of this chapter is to discuss the nature and role of military cyber operations. The chapter proceeds in six parts. Part one provides a glimpse at the evolving scholarly study of cyber operations. Part two conceptualizes military cyber operations in the present and explains the different forms of operations and operational processes. Part three examines the distinct features of cyber operations and how these features differ from or are similar to more conventional military operations. Part four, in turn, explains to what degree cyber operations can be used as a tool of coercion. Part five examines the potential for conflict

A. Brantly
Department of Political Science, Virginia Tech, Blacksburg, VA, USA
e-mail: abrantly@vt.edu

M. Smeets (✉)
Center for Security Studies, ETH Zurich, Zurich, Switzerland
e-mail: max.smeets@sipo.gess.ethz.ch; Mwsmeets@stanford.edu

A. Sookermany (ed.), *Handbook of Military Sciences*,
https://doi.org/10.1007/978-3-030-02866-4_19-1

escalation in cyberspace and beyond. The chapter concludes with a brief discussion drawing together the disparate themes introduced.

Keywords

Military cyber operations · Vulnerability · Cyber conflict · Cyber war · Deterrence · Threat

Introduction

Over the years, experts – both in and outside of the military – have repeatedly stated that we need to improve our conceptual and doctrinal thinking when it comes to military cyber operations and how to address the cyber threat (For a similar statement see: Smeets 2018). "It's 1946 in cyber," according to James Mulvenon. "We have these potent new weapons, but we don't have all the conceptual and doctrinal thinking, that supports those weapons or any kind of deterrence" (Singer and Friedman 2014). In 2010, when Gen. Keith Alexander went to lead the NSA and US Cyber Command, he uttered that there is "much unchartered territory in the world of cyber policy, law and doctrine" (United States Senate Armed Services Committee 2010). In 2014, when Michael Rogers followed up Keith Alexander to lead US Cyber Command, he made a similar statement: "We as a military and a nation are not well positioned to deal with [. . .] the changing threat in cyberspace" (United States Senate Armed Services Committee 2014). Four years later, in 2018, General Paul Nakasone, the new head of US Cyber Command and NSA continued the sentiment: "What we have to do is continue to determine what is the best way forward here, what fits within our national strategy, and then act on that" (United States Senate Armed Services Committee 2018).

From Cyber Pearl Harbor to Cyber Bombs and Beyond

The study of cyber operations has been evolving in its modern scholarly form since at least 1993 when John Arquilla and Dave Ronfeldt first wrote a RAND report on the changing nature of conflict and the kinds of military structures and doctrines what would be needed in the future (Arquilla and Ronfeldt 1993). However, modern connotations aside, the history of operations occurring in and through the Internet and networked computers predates Arquilla and Ronfeldt and took up prominence within military and national security concerns beginning in the 1960s (Warner 2012). Many computer and early Internet security concerns took a back stage to other issues at the end of the Cold War, but it was the release of the 1983 science fiction film *WarGames* starring Matthew Broderick as a nerdy teen who in the process of hacking into computer game companies accidentally initiates a countdown to an actual nuclear launch that sets discussions and concerns of modern cybersecurity on their current trajectory. Modern cybersecurity concerns as a

significant threat arose when President Reagan upon watching the film at the White House queried his military and national security leadership as to the feasibility of the film and was unpleasantly surprised to learn that the reality was actually worse than science fiction (Kaplan 2016).

In the years that followed the release of WarGames, the US government began enacting laws and building structures to ensure the protection of government computers and systems connected through the evolving MILnet and NSFnets and later the Internet. As networks of interlinked computers increasingly pervaded the public and the private sectors of nearly all countries on earth, fears that vulnerabilities within these networks constituted existential threats increasingly rose to prominence both within academia and beyond. These fears culminated in a term coined by John Markoff, a New York Times reporter, who wrote of a "electronic Pearl Harbor" (Lawson and Middleton 2019). The term stuck and became enmeshed within general scholarly vernacular as the potential for a "Cyber Pearl Harbor." Further credence was added to the term when in 2012 US Secretary of Defense Leon Panetta also spoke of a potential crippling "Cyber Pearl Harbor" (Ibid.).

The hyperbolic nature of the concept of a potential Cyber Pearl Harbor resulted in several works pushing back against the utility of the term and the reality of the impact of cyber conflict within military operations. Most significant among these works was an article by Thomas Rid, entitled "Cyber War Will Not Take Place" (Rid 2012). Despite the consistent utilization of hyperbole within a variety of scholarly and journalistic works on cyber operations (Kello 2017), an increasingly large volume of scholarship sought to parse out the mechanisms of conflict within cyberspace and in so doing isolate factors relating to the organization, utilization, and effect of cyber operations (Lin 2012; Kramer et al. 2009). The trajectory of scholarship on cyber operations has largely been divided into two principal camps diverging on perceived impacts. Generally, the field interprets impacts by following one of two courses of scholarship emphasizing nuance or hyperbole. Scholars focused on nuance privilege data-driven retrospective analyses, while those privileging hyperbole often focus on future oriented prognostications that extrapolate on potentialities. Below in our analysis of cyber operations, we focus on data-driven retrospective analysis that leverages existing cases and structures to identify and outline the contours of military cyber operations broadly.

Conceptualizing Military Cyber Operations

Military cyber operations can be defined as those cyber operations which a military entity of a nation-state plans and conducts to achieve strategic, operational, or tactical gain. (This means that the definition of military cyber operations is entity rather than effect dependent. Not all cyber effects operations are necessarily military operations – and vice versa.) A common distinction is made between three types of operations: (i) defensive cyber operations, those actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within a governments information systems and computer

Table 1 Stages of a cyber operation

	Stage	Description
1	Reconnaissance	Research, identification, and selection of targets
2	Weaponization	Pairing remote access malware with exploit into a deliverable payload
3	Delivery	Transmission of weapon to target
4	Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
5	Installation	The weapon installs a backdoor on a target's system allowing persistent access
6	Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network
7	Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.

networks; (ii) cyber espionage operations, those actions taken through the use of computer networks to gather data from target or adversary information systems or network; and (iii) offensive cyber operations, those actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves, or in basic, operations designed to achieve tangible effects (These definitions are adopted based on the US Department of Defense classic distinction between Computer Network Attack, Computer Network Defense and Computer Network Exploitation and align with Joint Publication 3-12 on Cyberspace Operations).

In much the same way as conventional military operations have squad, platoon, and company, cyber teams are comprised a diverse set of individuals each bringing skills to bear in cyber operations. Teams are oriented towards one of the three types of military cyber operations listed above. And in many countries, members of teams will rotate between operation types over the course of their career to gain or improve upon necessary skills.

Cyber operations are comprised of several stages, largely dependent on type and objective of the operation. These stages are summarized in Table 1 and align with Lockheed Martin's Kill Chain Model. (There are several frameworks which lay out the stages of a cyberattack. This chapter draws on a common framework called the "Kill Chain" from Lockheed Martin. An alternative framework is MITRE's ATT&CK framework.) The first stage, or *reconnaissance* stage, involves activities to understand which targets will enable the operator to meet the objectives. This could include planning activities such as identifying employees of a company on social media networks or harvest email addresses. The second stage is the weaponization phase in which military cyber teams actively prepare for the operation. For example, teams work on selecting and compiling a backdoor and appropriate command and control infrastructure of the operation. Third, at the *delivery* stage the cyber team seeks to convey the malware to the target – it is the actual launch stage of an operation. Delivery of malware can occur through a malicious email, USB stick, or a man-in-the-middle attack among a variety of other potential attack vectors. Fourth, the *exploitation* phase is when the cyber team exploits

a vulnerability to gain access. This could be software, hardware, or human vulnerability. Fifth, the *installation* phase is when the team installs a backdoor or implants in the target environment to maintain access. Sixth, during the Command & Control (C2) phase, the team opens a command channel control the implants and remotely manipulate the target network or system. Seventh, at the final stage of actions and objectives, the attack achieves the ultimate mission's goal. An example of a goal could be the collection of user credentials, destruction of systems, or the modification of data.

These stages illustrate that there are close similarities between different forms of cyber operations. Indeed, as former NSA and CIA Director Michael Hayden writes about the connection between cyber espionage operations and cyber effects operations: "Reconnaissance should come first in the cyber domain too. How else would you know what to hit, how, when - without collateral damage? But here's the difference. In the cyber domain reconnaissance is usually a more difficult task than the follow-on operation. The difficulty resides in the technical reality that it is often tougher to penetrate a network and reside on it undetected while extracting large volumes of data from it than it is to, digitally speaking, kick in the front door and fry a circuit or two. [...] For example, an attack on a network to degrade it or destroy information in it is generally a lesser included case of the technology and operational art needed to spy on that same network" (Hayden 2016). Breaking into and subsequently on a system, subtly manipulating that system for espionage collection and eventually degrading, damaging all while avoiding automated and human detection requires substantial skill and actors with this level of capability are often referred to as advanced persistent threats.

In addition, it is important to recognize that the extensive planning of military cyber operations. Cyber operations are not conducted at the speed of light – operational planning takes time, dedication, and effort. As James McGhee states, "While we may have some number of cyber capabilities 'on the shelf', their operational use requires much more than simply loading them and sending them on their way. Our operators must first know and understand the target network, node, router, server, and switch before using any cyber capability against them" (McGhee 2016). Furthermore, as Ben Buchanan elaborates that "the speed of an operation varies by step; operational steps are linear but without strong momentum; persistence is powerful; and parts of operations can be prepared in advance" (Buchanan 2017).

Until very recently under Presidential Policy Directive 20 (PPD-20), a still classified document leaked by NSA contractor Edward Snowden, required military cyber teams in the United States to seek substantial review from various levels of government, including presidential authorization. PPD-20 has since been overwritten by the Trump administration in such a way as to ease the oversight constraints placed on teams (Council on Foreign Relations 2018). It is likely that many other nations based on their doctrines and their organizations structures have similar oversight or bureaucratic requirements that constrain the use of offensive cyber operations. These constrains add legal and policy barriers to the already arduous technical challenges ever-present within cyberspace.

Dimensions of Military Cyber Operations

Much has been written on the distinct features of cyber operations – distinguishing operations in cyberspace from operations in the conventional domain (For an excellent overview see: Owens et al. 2009; S-1, Sects. 1.4 and 2.1). First, cyber operations are often undertaken with the assumption of high degrees of anonymity (Brantly 2016). The obscurity of the identity and location of actors is frequently referred to as the "attribution problem." According to Herb Lin, attribution can have three meanings. First, attribution can be defined as ascertaining the machines associated with a cyberattack. Second, attribution can be defined as ascertaining the identity of the person or persons directly involved in conducting the cyber operation. Third, attribution can be defined as ascertaining the ultimate responsible part of a cyberattack. Attribution at this level is less about "who did it?" and more about "who's to blame?" Responsibility is context dependent and not a binary phenomenon. Defenders often triangulate a variety of indicators to provide a probabilistic assessment of actor attribution (Brantly 2015). Healey has outlined a spectrum of state responsibility to more precisely assign responsibility for a cyberattack (Healey 2011). Table 2 lists the 10 categories on the spectrum, each marked by a different degree of state responsibility based on whether a state ignores, abets, or conducts a cyber operation.

Attribution is as much and art as a science. As Ben Buchanan and Thomas Rid note, "There is no one recipe for correct attribution, no one methodology or flowchart or check-list. Finding the right clues requires a disciplined focus on a set of detailed questions — but also the intuition of technically experienced operators. It requires coup d'œil, to use a well-established military term of art. On an

Table 2 The spectrum of national responsibility for cyber operations

1	**State-prohibited**	The national government will help stop the third-party attack
2	**State-prohibited-but-inadequate**	The national government is cooperative but unable to stop the third-party attack
3	**State-ignored**	The national government knows about the third-party attacks but is unwilling to take any official action
4	**State-encouraged**	Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5	**State-shaped**	Third parties control and conduct the attack, but the state provides some support
6	**State-coordinated**	The national government coordinates third-party attackers such as by "suggesting" operational details
7	**State-ordered**	The national government directs third-party proxies to conduct the attack on its behalf
8	**State-rogue-conducted**	Out-of-control elements of cyber forces of the national government conduct the attack
9	**State-executed**	The national government conducts the attack using cyber forces under their direct control
10	**State-integrated**	The national government attacks using integrated third-party proxies and government cyber forces

Table 3 Cyber operations collateral effects, mitigating actions, and representative controls

Undesired collateral effects	Mitigating actions	Representative controls
Unintended infection	Limit propagation to specific targets	1. Disallow self-replication 2. Infect systems only via spear phishing with malicious attachment or link to download or through previously infected systems
Unintended payload execution causing loss of: a. Confidentiality (data exposure) b. Availability (loss of data, denial of service, consumption of network resources) c. Integrity (data modification)	Prevent payload execution on nontarget systems	1. Use only active control measures to activate payload 2. Use detailed reconnaissance to determine triggers for passive or hybrid control 3. Trigger malware based on known target configuration
Vulnerability disclosure to unintended individuals or general public	Prevent reverse engineering and subvert forensic investigation	1. Encryption 2. Tamper protection 3. Temporary payloads that delete themselves from memory
Attribution of attack or source of the malware	Eliminate evidence of authors	1. Encryption 2. Tamper protection 3. Use widely used languages, libraries, and coding techniques 4. Temporary payloads

operational level, attribution is a nuanced process, not a simple problem. That process of attribution is not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades" (Rid and Buchanan 2015).

Second, military cyber operations are thought to have a higher risk of collateral damage. This does not mean, however, that military cyber operations are inherently indiscriminate. Cyber operations can be undertaken in a targeted manner – though it often makes the process more technically demanding and increased the amount of intelligence required about the target networks and/or systems. But, as Bellovin, Lin and Landau note, "When the technical demands can be met and the requisite intelligence is in hand, it is possible to conduct cyberattacks that are precisely targeted to achieve a desired effect and with minimal damage to entities that should remain unharmed." (The scholars use the term "cyber weapon" instead of military cyber operation.) An excellent framework on the type of collateral effects and how they can be mitigated or repressed is developed by Raymond et al. (2013). The framework is shown in Table 3.

Briefly mentioned, but deserving of additional attention, is the notion of reverse engineering of malware used by military cyber operations teams. When bullets or missiles are fired, their ability to be reconstituted and returned to sender a limited. Yet, time and again the development and use of malware by militaries and intelligence agencies have resulted attacks that have leveraged the originating attackers own code. Examples abound, but one of the more prominent incidents in recent years

was the use of Eternalblue exploit developed by the NSA and subsequently implemented in the WannaCry attacks that crippled hospital systems globally including the NHS in the United Kingdom (Greenberg 2019). The reconstitution of malware by other state actors is a serious threat, that can and has impacted original attacking parties as well as third-parties not engaged in initial cyber operations. Knowing that code, unlike kinetic weapons, can be reused, should give pause both to the developers of exploits as well as those using them in military operations. Even a precisely targeted attack can and often does leave behind sufficient forensic data for the discovery of the attacking exploits attributes to be reverse engineered. This challenge places military cyber operations in a difficult position often referred to as the vulnerabilities and equities process in which they must weigh the costs and benefits of cyber operations beyond the first use of an exploit.

Third, cyber operations are transitory in nature: they are strongly time dependent in terms of their potential to cause harm to targeted systems (Smeets 2017; Smeets and Work 2020). The transitory nature of cyber operations is both a technical and a social product. Actors greatly differ in their ability to execute cyber operations. Certain actors have a wider variety of exploits and implants at their disposal, enabling more targeted attacks and thus reducing the chances of discovery. Also, the time-consuming process of developing and conducting operations leads to "constant trade-offs between the skills and resources required to develop a new computer code, and the odds of successfully penetrating targeted systems." Offensive actors also have to make trade-offs with respect to the deployment of exploits and implants. Using a capability against a higher number of targets increases its chances of discovery. The type of targets matters too: not every actor has equal ability to detect and expose an attack. In some cases, it is much more likely the attack will go unnoticed (Ibid.).

Can Military Cyber Operations Coerce?

Numerous national strategies talk about the increasing role of offensive cyber operations; it is hardly surprising that coercion has received a great deal of attention. (Following Shelling, coercion in this context refers to both deterrence and compellence. Shelling 1966) Whereas there are few works on compellence, a large number of models have been proposed on how cyberattacks can be deterred by an adversary through the (threatened) use of a broad set of means (Borghard and Lonergan 2017). Most of the published articles argue that while it is more difficult to deter cyberattacks, there are ways policymakers can dissuade actors from attacking (Lindsay 2015; Libicki 2009). For example, Uri Tor proposes the notion of cumulative cyber deterrence: we should not seek to deter individual attacks but a series of attacks (Tor 2017). Joseph Nye Jr. notes that conventional cyber deterrence is difficult, but policymakers could instead focus on deterrence by economic entanglement and norms to overcome barriers (Nye 2016/2017). A more detailed overview of recent positions of scholars on cyber deterrence can be found in Table 4 (The scholars note that "Studies of 'cyber deterrence' raise as many problems as

Table 4 Overview of scholars' arguments on the potential to deter cyberattacks

Denning	Same problems for CD as for conventional deterrence. Potential for CD through existing regimes
Brantly	Absolute deterrence may not be possible – but a form deterrence as in criminology might be. We need to move away from deterrence only by punishment and denial
Healey	CD is still working on the high-end – yet, nations show limited restraint. It is the aspect of "constant cyber activity" which causes problems
Nye	Conventional CD is difficult. Instead, we should focus on deterrence by economic entanglement and norms to overcome barriers
Sulmeyer	CD might be possible in theory. However, we are still unclear what activity to deter, and which tools to use to impose costs
Stevens and Muller	(NATO) CD seems to be viable. Yet, it should be viewed as a cumulative process, beyond military
Kello	CD does not work as a strategy, but we should aim for punctuated CD instead: we should not deter individual actions but a series of actions
Tor	We should move from "absolute" CD to "cumulative" CD, which is restrictive and continuous in nature
Lindsay and Gartzke	CD suffers from problems of rationality, attribution, and secrecy. This means we have to instead focus on deception as distinct strategy
Harknett	CD is impossible due to the structure of cyberspace. We there need to move away from the deterrence paradigm and consider different forms of strategy

would be raised by a comparable study of 'land deterrence'." Denning 2015; ibid.; Nye 2016/2017; Ibid.; Kello 2017; Tor 2017; Harknett and Nye 2017; Also see William 2017; Harknett and Fischerkeller 2017; Brantly 2018; Harknett and Smeets 2020).

Yet, this leaves open the question to what degree cyber operations can be used to deter a certain type of (military) means of an adversary (rather than whether some type of means can be used to deter a cyberattack). The transitory and clandestine nature of cyber operations makes it difficult to prove you have a specific type of capability predeployment. This means state actors can talk about specific military cyber capabilities whether or not they actually have them. Since possession is hard to verify, such talk can be described as "cheap talk" (Farrell and Rabin 1996; Thyne 2006; Farrell and Gibbons 1989).

Hence, state actors can talk about offensive cyber capabilities whether or not they actually have them; such talk is intended to convey to other actors the impression that the talking nation does have the talked-about capabilities (For a more detailed discussion see: Smeets and Lin 2018a). But since the fact of possession cannot be verified by other actors nor demonstrated by the talking state, such talk is cheap talk. Yet, cheap talk can still be meaningful in certain circumstances – especially if an actor has a certain reputation and credibility on the intention and ability to conduct an offensive cyber operation. As Smeets and Lin "[t]his has led to a number of paradoxical dynamics for cyber conflict." "The release of the classified National Security Agency (NSA) documents by Edward Snowden has been described as the most embarrassing episode in the history of the secretive US intelligence agency.

It revealed how the NSA maintained a mass surveillance program over its own citizens, accessed data from companies, intercepted data from global communications networks and stored information of millions of people. Yet, it also exposed the impressive arsenal of the agency," the scholars state (Ibid. Also see: Gompert and Libicki 2015; also see Libicki 2016, p. 198).

More specifically, Erica Borghard and Shawn Lonegran argue that three uses of military cyber power are most likely to be useful for aspiring coercers in cyberspace: (i) attrition, a strategy which aims to erode the adversary's military capability such that the target can no longer resist, (ii) denial, a strategy which aims to increase the costs to an adversary such that achieving a military objective – such as taking a piece of territory – becomes prohibitive or impossible; (iii) and decapitation, a strategy which aims to achieve strategic paralysis by targeting command and control centers, leadership, critical economic nodes, and key weapons systems. The scholars argue that a strategy of punishment is more difficult for cyber operations, as the scale and scope required to inflict severe costs on enemy populations is hard to achieve. The scholars also argue that "risk strategies" – those strategies which gradually escalating the intensity and scope of attacks against civilian targets – are more difficult to pursue for military cyber operations. A tiered cyber campaign plan creating a ratcheting effect is difficult, as defense is said to become easier over time, and "effects can get beyond the control of the initiating state in unanticipated and potentially undesirable ways" (Borghard and Lonergan 2017).

Risks of Escalation

Concurrent to coercion is escalation. As states deter and coerce, they also seek to manage how quickly conditions change and often seek to maintain escalation dominance (Byman and Waxman 2001). As noted by Martin Libicki "in cyberspace, such calculations are particularly complex" (Libicki 2012), Libicki goes on to assess that many of the challenges associated with the management of escalation in cyberspace revolve around perceptions of gaining military advantage. Moreover, he states that while anonymity is maintained, the risk of escalation in nearly all activities constituting the preparation of the "cyberbattlefield" is limited. But escalation in cyberspace occurs within a digital fog of war between operators often engaging one another at great distances with stealth and subterfuge. Knowing where the line between status quo and escalation is can be nearly impossible until it has already been crossed. Moreover, as was discussed in the previous sections, many of the activities leading up to offensive actions in cyberspace that degrade, deny, destroy, or otherwise damage computers, information, or affiliated systems are undertaken clandestinely. Whereas in conventional conflict it is potentially possible with intelligence assets to ascertain the movement of armies and navies as they move into position, in cyberspace it is very likely the opposing force has already been in your system for quite some time.

The risks attendant with military cyber operations do, however, in many ways parallel the risks associated with conventional effects based military operations.

Comparable damage and destruction to critical infrastructure can be wrought with kinetic and cyber weapons. Through the manipulation of nuclear power plants, it is also conceivable that cyber operations might even result in radiological effects (Futter 2018). Yet for all their escalatory potential, the data on escalation in cyberspace to date is less than clear. Sarah Kreps and Jacquelyn Schneider, following detailed analysis and in line with historical analysis on firebreaks differentiating conventional and nuclear weapons, likewise find a firebreak of sorts between cyber and conventional and nuclear (Sarah Kreps and Schneider 2019). Their study finds that members of the general public and decision-makers identify in cyber operations something that is categorically different from conventional and nuclear operations and are consequently unwilling to retaliate let alone escalate (Ibid.). This firebreak highlights a cognitive disconnect between actions taken in cyberspace and those taken outside of it. While the same outcomes might occur, these outcomes are processed or interpreted in different ways. Kreps and Schneider write: "Our study suggests that cyberattacks create a threshold that restrains the escalation of conflict. Americans are less likely to support retaliation with force when the scenario involves a cyberattack even when they perceive the magnitude of attacks across domains to be comparable. Our findings provide support for cyber strategies based on assumptions of cyber thresholds, while also casting doubt on the credibility of cyber deterrence by punishment. More broadly, our research suggests effects-based theories of escalation may not help understand the impact of emerging technologies on strategic stability" (Ibid.). These findings both limit the escalatory potential of cyberattacks and constrain their utility, a finding reiterated below by Borghard and Lonergan.

Analysis by Brandon Valeriano, Benjamin Jensen, and Ryan Maness highlights a distinct lack of escalation within cyberspace related to offensive cyber operations (Valeriano et al. 2018). Valeriano et al. contend that cyber operations serve as a release valve that prevents escalatory behaviors in other domains. Their detailed data on hundreds of cyber incidences over the past two decades indicates no clear escalatory patterns. Moreover Valeriano et al. note: "The ambiguity of cyberspace shields decision makers from hawks, who will demand higher rates of escalation, and doves, who will demand appeasement" (Ibid.). In all of their cases, they documented only two instances of escalation, both related to Stuxnet. Their data paired with that of Kreps and Schneider indicate that cyberspace is a potentially highly permissive environment in which actions can occur with little consequence.

Borghard and Lonergan writing on the exaggerated nature of escalation in cyberspace: "... if cyberspace is in fact an environment that (perhaps even more so than others) generates severe escalation risks, why has cyber escalation not yet occurred? Most interactions between cyber rivals have been characterized by limited volleys that have not escalated beyond nuisance levels and have been largely contained be- low the use-of-force threshold" (Borghard and Lonergan 2019). Borghard and Lonergan continue in writing by outlining three principal reasons why escalation is rare in cyberspace: First, retaliatory offensive cyber operations may not exist at the desired time of employment. Second, even under conditions where they may exist, their effects are uncertain and often relatively limited. Third, several attributes of offensive cyber operations generate important trade-offs for

decision-makers that may make them hesitant to employ capabilities in some circumstances. Finally, the alternative of cross-domain escalation – responding to a cyber incident with noncyber, kinetic instruments – is unlikely to be chosen except under rare circumstances, given the limited cost-generation potential offensive cyber operations" (Ibid.). Combined the evidence of escalatory potential in cyberspace seems to indicate that cyber operations while rhetorically portrayed as a wild west of state to state interactions exhibit patterns of behavior that are less bellicose and more measured. If states and their militaries are more measured, should we be concerned with escalation?

While the evidence to date indicates limited evidence of escalation in response to cyber operations, two authors in particular highlight that the potential for escalation should not be ignored. Libicki, writing prior to the release of the 2018 DoD Cyber Strategy revision, highlighted a number of ways in which conflict in cyberspace whether due to attributional issues or ineffective information on signaling intent might lead states to escalate in response to cyberattacks (Libicki 2012). Libicki further notes understanding and managing an escalation ladder requires understanding how a potential adversary will respond. Such an understanding is largely absent in cyberspace, in part because of a lack of clarity on capabilities of the adversary as well as a lack of understanding of one's own vulnerabilities to within domain escalation. Whereas conventional intelligence is highly useful in assessing and understanding the kinetic capability of adversaries, the comparable assessment of cyber capabilities is only discovered through leaks or unintentional disclosures.

The challenges and risks associated with managing escalatory behaviors in cyberspace are further reiterated by Jason Healey who finds that the very strategy of persistent engagement makes some fundamental assumptions about adversary behavior which might be wrong (Healey 2019; also see Smeets and Lin 2018b). Such an underestimation is potentially risky in dyadic interactions. Yet the risks increase markedly when other actors, emulating the US strategic posture, also engage in persistent engagement. The potential risks associated with multiple actors all engaging in concurrent cyber operations increase the potential for miscalculation.

Discussion: The Evolving Nature of Military Cyber Operations

Military operations in cyberspace, while not entirely new, having been initiated in the 1990s, are only now coming into their own. As quotes by General Nakasone and others illustrate, states, in particular the United States, are increasingly viewing cyberspace as a valid domain of military action and are structuring their military forces, developing legal and policy frameworks, actively engaging in operations. This chapter has highlighted the contours of a field of inquiry and a practice that is changing rapidly. New questions, new capabilities, and ominously more and more targets are coming online in cyberspace. The result is that operations to defend, surveil, and engage in offensive activities in cyberspace are in many ways still in

their nascent stages. In the span of 30 years, more than 3 billion people have come online. Nearly every country in the world has some form of critical infrastructure that relies on the Internet. Developed countries are increasingly wholly dependent on cyberspace for everything from the management of national security command and control, to the functioning of streetlights and the cars on roads.

An increasing number of countries are actively seeking to fund and train military cyber operators. Prominent actors with cyber programs today include the United States, Russia, Iran, China, North Korea, Israel, Netherlands, Estonia, the United Kingdom, and many more. Just as states learned to effectively wield other technologies from machine guns and tanks, to strategic aircraft and ballistic missiles, states are actively engaging one another and learning how to wield the potential of cyberspace to their advantage. Whether learning where deterrence works, or doesn't, or when states will or will not escalate in response to cyberattacks, the future of military cyber operations is evolving. As challenges such as attribution are increasingly addressed, and as new technologies such as artificial intelligence, machine learning, quantum cryptography, and other technologies improve, militaries will have to adapt to remain relevant and effective. The one constant of cyberspace is that it is growing ever more important to the economic, political, and social well-being of states and their citizens, the result is that military cyber operations to safeguard states, and their citizens will continue to grow in importance in the coming decades.

Summary

This chapter discusses the nature and role of military operations in cyberspace. The chapter proceeds in six parts. Part one provides a glimpse at the evolving scholarly study of cyber operations. Part two conceptualizes military cyber operations in the present and explains the different forms of operations and operational processes. Part three examines the distinct features of cyber operations and how these features differ from or are similar to more conventional military operations. Part four, in turn, explains to what degree cyber operations can be used as a tool of coercion. Part five examines the potential for conflict escalation in cyberspace and beyond. The chapter concludes with a brief discussion drawing together the disparate themes introduced.

References

Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar is Coming!*. Santa Monica: RAND Corporation. https://www.rand.org/pubs/reprints/RP223.html

Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies, 26*(3), 452–481.

Borghard, E., & Lonergan, S. (2019). Cyber operations as imperfect tools of escalation. *Strategic Studies Quarterly, 13*(3), 123.

Brantly, A. F. (2015). Aesop's wolves: The deceptive appearance of espionage and attacks in cyberspace. *Intelligence and National Security, 31*(5), 674–685. https://doi.org/10.1080/02684527.2015.1077620.

Brantly, A. F. (2016). *The decision to attack: Military and intelligence cyber decision-making* (pp. 79–89). Athens: University of Georgia Press.

Brantly, A. (2018). The cyber deterrence problem. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), *10th international conference on cyber conflict.* Tallinn: NATO CCD COE Publications. Retrieved from: https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf

Buchanan, B. (2017). *Cybersecurity dilemma* (p. 41). Oxford: Oxford University Press

Byman, D., & Waxman, M. C. (2001). *The dynamics of coercion: American Foreign Policy and the limits of military might* (Rand studies in policy analysis). New York: Cambridge University Press.

Council on Foreign Relations. (2018). What do the trump administration's changes to Ppd-20 mean for U.S. offensive cyber operations? https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations. Accessed 1 May 2020.

Denning, D. E. (2015). Rethinking the cyber domain and deterrence. *Joint Forces Quarterly, 77,* 15. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq77/jfq-77_8-15_Denning.pdf

Farrell, J., & Gibbons, R. (1989). Cheap talk with two audiences. *The American Economic Review, 79*(5), 1214–1223.

Farrell, J., & Rabin, M. (1996). Cheap talk. *Journal of Economic Perspectives, 10*(3), 103–118.

Futter, A. (2018). *Hacking the bomb: Cyber threats and nuclear weapons*. Washington, DC: Georgetown University Press.

Gompert, D. C., & Libicki, M. (2015). Waging cyber war the American way. *Survival, 57*(4), 7–28.

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. New York: Doubleday.

Harknett, R. J., & Fischerkeller, M. P. (2017). Deterrence is not a credible strategy for cyberspace. *Orbis, 61*(3), 381393.

Harknett, R. J., & Nye, J. S. (2017). Is deterrence possible in cyberspace? *International Security, 42*(2), 196–199.

Harknett, R. J., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/01402390.2020.1732354

Hayden, M. (2016). *Playing to the edge: American intelligence in the age of terror* (p. 137). New York: Penguin Random House.

Healey, J. (2011). The spectrum of national responsibility for cyberattacks. *The Brown Journal of World Affairs, 18*(1), 57–70. www.jstor.org/stable/24590776

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity, 5*(1). https://doi.org/10.1093/cybsec/tyz008.

Kaplan, F. M. (2016). *Dark territory: The secret history of cyber war*. New York: Simon & Schuster.

Kello, L. (2017). *The virtual weapon and international order*. New Haven: Yale University Press.

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyberpower and national security*. Washington, DC: Potomac.

Lawson, S., & Middleton, M. K. (2019). Cyber pearl harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991–2016. *First Monday, 24*(3). https://doi.org/10.5210/fm.v24i3.9623.

Libicki, M. C. (2012). *Crisis and escalation in cyberspace*. Santa Monica: RAND Corporation. https://www.rand.org/pubs/monographs/MG1215.html

Libicki, M. (2016). *Cyberspace in peace and war* (p. 198). Annapolis: Naval Institute Press.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, Rand Corporation.

Lin, H. S. (2012). Operational considerations in cyber attack and cyber exploitation. In D. S. Reveron (Ed.), *Cyberspace and national security*. Washington, DC: Georgetown University Press.

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity, 1*(1), 53–67.

McGhee, J. (2016). Liberating cyber offense. *Strategic Studies Quarterly, 10*(4), 46–63.

Nye, J. S. (2016/2017). Deterrence and dissuasion in cyberspace. *International Security, 43*(3): 44–71.

Owens, W. A., Dam, K. W., & Lin, H. S. (Eds.) (2009). *Excerpts from technology, policy, law and ethics regarding U.S. acquisition and use of cyberattack capabilities*. Washington DC: National Research Council.

Raymond, D., Conti, G., Cross, T., & Fanelli, R. (2013). A control measure framework to limit collateral damaga and propagation of cyber weapons. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *2013 5th international conference on cyber conflict.* Tallinn: © NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/8_d1r2s6_raymond.pdf; http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=67E85114AA1D5C3942296FA224578088?doi=10.1.1.385.7204&rep=rep1&type=pdf

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.

Sarah Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity, 5*(1), 1–11.

Shelling, T. (1966). *Arms and influence*. New Haven: Yale University Press.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. New York: Oxford University Press.

Smeets, M. (2017). On the transitory nature of cyber weapons. *Journal of Strategic Studies, 1*, 28.

Smeets, M. (2018). The strategic promise of offensive cyber operations. *Strategic Studies Quarterly, 12*, 90–113.

Smeets, M., & Lin, H. S. (2018a). Offensive cyber capabilities: To what ends? In T. Minárik, R. Jakschis, & L. Lindström (Eds.), *2018 10th international conference on cyber conflict, CyCon X: Maximizing effects*. Tallinn: NATO CCD COE Publications.

Smeets, M., & Lin, H. S. (2018b). A strategic assessment of the US Cyber Command vision. In *Bytes, bombs, and spies: The strategic dimensions of offensive cyber operations*. Washington, DC: Brookings Institution Press.

Smeets, M., & Work, J. D. (2020). Operational decision-making for cyber operations: In search of a model. *Cyber Defense Review, 5*(1), 95–112.

Thyne, C. L. (2006). Cheap signals with costly consequences: The effect of interstate relations on civil war. *Journal of Conflict Resolution, 50*(6), 937–961.

Tor, U. (2017). 'Cumulative deterrence' as a new paradigm for cyber deterrence. *Journal of Strategic Studies, 40*(1–2), 92–117.

United States Senate Armed Services Committee. (2010). Stenographic Transcript before the Committee on Armed Services United States Senate Nominations General Keith Alexander," U.S. Senate Committee on Armed Services, April 15, 2010. www.armed-services.senate.gov

United States Senate Armed Services Committee. (2014). Advance questions for vice admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command, March, 11 2014, pp. 7–8. www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf

United States Senate Armed Services Committee. (2018). Stenographic Transcript before the Committee on Armed Services United States Senate Nominations for Lieutenant General Paul Nakasone to be Commander of the U.S. Cyber Command and Director of the National Security Agency and Chief of the Central Security Service, March 1, 2018. https://assets.documentcloud.org/documents/4407097/United-States-Senate-Armed-Services-Committee.pdf

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford: Oxford University Press.

Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security, 27*(5), 781–799.

William, B. D. (2017, July 19). Meet the scholar challenging the cyber deterrence paradigm. *The Fifth Domain*. Retrieved from https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/