NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBER WEAPONS AND DETERRENCE

by

Elizabeth E. Wanic

September 2018

Thesis Advisor:	Neil C. Rowe
Second Readers:	Dorothy E. Denning
	Ryan Maness

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE CYBER WEAPONS AND DETERRENCE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Elizabeth E. Wanic	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

With the increasing frequency of cyberattacks, there has been growing discussion on whether these actions can be deterred, and if so, how it can be accomplished. At the same time, there is a lack of international agreement on norms and standards for the use and development of cyber weapons. This thesis examines existing deterrence theory and addresses ts applicability in cyberspace. It describes differences between cyber weapons and conventional weapons and outlines the implications these differences can have on the effectiveness of cyber weapons as a deterrent. Expected outcomes of the cyber operation actions taken by the United States and its adversaries, including Russia, China, Iran, and North Korea, are highlighted. Possible actions with a potential deterrence effect are discussed, including stockpiling cyber weapons, using deception, imposing sanctions, creating international agreements, retaliating with conventional weapons, improving defenses, developing automated counterattack mechanisms, and mounting offensive cyber actions. The effectiveness of these actions as deterrents to adversaries and recommendations for U.S. policy are made.

14. SUBJECT TERMS cyber weapons, cyber deterrence, policy, cyber norms	**15. NUMBER OF PAGES** 51
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

CYBER WEAPONS AND DETERRENCE

Elizabeth E. Wanic
Civilian, Federal Cyber Corps
BA, Butler University, 2003
MS, City College of New York, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2018

Approved by: Neil C. Rowe
Advisor

Dorothy E. Denning
Second Reader

Ryan Maness
Second Reader

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

With the increasing frequency of cyberattacks, there has been growing discussion on whether these actions can be deterred, and if so, how it can be accomplished. At the same time, there is a lack of international agreement on norms and standards for the use and development of cyber weapons. This thesis examines existing deterrence theory and addresses its applicability in cyberspace. It describes differences between cyber weapons and conventional weapons and outlines the implications these differences can have on the effectiveness of cyber weapons as a deterrent. Expected outcomes of the cyber operation actions taken by the United States and its adversaries, including Russia, China, Iran, and North Korea, are highlighted. Possible actions with a potential deterrence effect are discussed, including stockpiling cyber weapons, using deception, imposing sanctions, creating international agreements, retaliating with conventional weapons, improving defenses, developing automated counterattack mechanisms, and mounting offensive cyber actions. The effectiveness of these actions as deterrents to adversaries and recommendations for U.S. policy are made.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Neil Rowe, for his guidance, direction and valuable discussions over the past year. Thank you for keeping me on track and focusing my thoughts. I would also like to thank my second readers, Dr. Dorothy Denning and Dr. Ryan Maness, for their helpful feedback and for finding the missing pieces. Additionally, I would like to thank my friends and family, including my sister and Youssef, for their support and patience during my time here at the Naval Postgraduate School. This journey was not always easy, but it was certainly worthwhile. While I would like mention everyone else by name, that list would be a thesis unto itself. I am grateful to you all.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

Computers, networked systems, and global interconnectivity have become integral to modern existence. However, along with efficiencies and other benefits, the prevalence of cyberspace across myriad sectors has also introduced new avenues for malicious actors to gain access to information and threaten critical components of national infrastructure. Therefore, protection of assets and maintenance of strength in infrastructure are an important aspect of the national security goals of a modern state (Libicki, 2016).

Throughout history, nations have striven to protect and maintain their power and defend their interests, personnel, and assets. Through diplomacy and alliances, demonstrations of strength, and stated policies, they have acted in strategic ways to let others know what consequences offensive actions might provoke in an effort to prevent conflict (Russet, 1963). As in other domains, nations seek to prevent adversaries from taking advantage of them in cyberspace, and seek to stop cyber actions, which would harm their interests. Therefore, examining how deterrence has succeeded and failed in cyberspace can provide guidance for national policy.

Existing deterrence strategies may seem to be partly effective, as we have not seen full-scale cyber warfare. For now, nations seem to be content with performing or condoning actions below the threshold of armed attack that do not invite escalatory retaliation (Libicki, 2016). However, if a Chinese cyberattack shut down the power of a United States (U.S.) military facility, they would expect the U.S. to respond. To date, there have been a few incidents that could have provoked retaliation but did not. One example is the Stuxnet attack against the Iranian Natanz nuclear enrichment facility, which has subsequently been attributed to the United States and Israel (Nakashima and Warrick, 2012). However, at the time it was discovered in 2010, attribution of cyberattacks was very difficult, and if Iran was not sure who to blame, against whom would they retaliate?

Major cyberattacks may have been avoided because they were expected and deterred, but it may be that the circumstances calling for their use have not yet occurred. Recent years, however, have seen an increase in other types of offensive cyber activity, including from nation-states. Perhaps potential attackers have deemed that lesser actions such as hacking private companies or email servers have more value to the achievement of their goals than outright cyber warfare. If so, then deterrence efforts should be rethought to cover these lesser attacks as well. Developing effective policies requires examination of attacker objectives and the means by which they intend to achieve them, along with an updating of our overall strategy.

B. OUTLINE OF THE THESIS

This thesis will look at deterrence in cyberspace in an effort to inform the discussion on its role in United States policy. Chapter II discusses deterrence theory and looks at its application in cyberspace. Chapter III outlines the main characteristics and strategies of the cyber operations of the U.S., Russia, China, North Korea, and Iran, including motivations behind and desired outcomes from these operations. Chapter IV suggests actions that can be taken by the United States to deter its adversaries from deploying their cyber capabilities against its interests. Lastly, Chapter V gives conclusions and addresses opportunities for future research.

II. DETERRENCE

A. DEFINING DETERRENCE

Deterrence can be defined as discouraging adversaries from taking an undesirable action against one's interests. It can be achieved through the threat of consequences or by fostering the perception that it will take too great an effort to achieve success (Snyder, 1959). Deterrence as a concept has been relevant as long as power dynamics have existed, but it has been discussed as a theory in its current canonical form most thoroughly for nuclear weapons and during the Cold War (Gerson, 2009). The concept of deterrence is a factor in strategy decisions and operational activities.

Employing the threat of consequences to deter adversary actions is usually termed deterrence by punishment (Snyder, 1959). This type of deterrence aims to cause an opposing force to believe that if they were to take certain actions, a counter-strike with severe negative effects would be forthcoming. It works best when the expected consequences would be so harsh that the gain from the prospective actions would be negated by the loss from the retaliation received. An example of deterrence by punishment was the buildup of armaments and military capabilities by the United States and Soviet Union during the Cold War. The prevailing logic was that the capacity to destroy the other would prevent either adversary from taking the first step.

Consequences can involve military action, sanctions, or loss of political standing. Retaliation may not necessarily be in kind, as for example a military action could result from a perceived political injury. Those with more to lose in the political arena may be more affected by political retaliation, while those with less military power might feel more threatened by an adversary that could devastate them militarily. Rogue states can be more difficult to deter, being less concerned about saving face than other states; as they are already outside of the norm, moving further from it often has little effect on them.

Most societies attempt to deter criminal behavior through the use of punishment. Convicted criminals are subject to monetary fines, prison or jail time, and in some cases, capital punishment. However, most evidence shows the deterrent effect is not strong and

increases in punishments do not correlate with decreases in crime (Libicki, 2009). While such deterrence efforts are aimed at individuals, the same strategies could be more effective against nation-states. As nations and their governments are aggregations of different psychologies, they tend to be more rational than individuals, who often act in more selfish or irrational ways (Kugler, Kausel, & Kocher, 2012).

Another method to deter aggression is to fortify your assets to a degree that the adversary must expend an unacceptable amount of energy, time, or resources to achieve their aims. This is known as deterrence by denial (Snyder, 1959). The adversary must assess that the amount of effort needed to achieve success is too great an expense to be paid, or that the return on investment for that action would be poor. Deterrence by denial does not require that the adversary be convinced of their ultimate defeat were they to enter into a contest, since "the deterrent effect is derived by convincing the aggressor that it cannot accomplish its objectives within an acceptable timeframe and cost" (Gerson, 2009, p. 40).

Extended deterrence is the concept that the deterrent capabilities of one state can deter actions against their allies as well (Gerson, 2009). The North Atlantic Treaty Organization (NATO) and other major alliances have functioned on this principal for many years. Extended deterrence can involve a stronger state protecting a weaker one, or multiple states protecting each other with complementary deterrent potential. For instance, it was not necessary for all Warsaw Pact nations to develop nuclear weapons, as it was understood that the Soviet Union arsenal could be deployed to retaliate for an attack on any member of the alliance.

It is useful to distinguish "red" and "blue" deterrence. Blue deterrence is said to be based around overtly specified rules that should apply equally to all actors, and promotes a worldview where value is placed on "the imposition of law over an anarchic world system" (Libicki, 2016, p. 337). The United States follows this perspective, which views deterrence as a foundation for international relations. To the blue way of thinking, the goal is stability, which can be achieved by "universal adherence to a set of norms" (Libicki, 2016, p. 339). Trouble arises when the lines specified by these norms are crossed, and deterrence aims to prevent such events. On the other hand, China is claimed

to exemplify red deterrence, focusing "on power, which, by definition, is relative" and their view is of "a world of hierarchy in which countries are of unequal power and patterns of deterrence reflect power relationships." From the red point of view, "deterrence is something one does to remind others of the need for respect" (Libicki, 2016, pp. 337–338).

The competing outlooks of red versus blue deterrence can cause miscalculations on either side. An agreement on norms may not have the desired outcome, as the red view may be that the rules should apply only to those without the power to act outside them, which is counter to the blue expectation that the rules apply to all. For example, China continues to assert its control over areas in the South China Sea regardless of international law, which has drawn it into disagreement with Vietnam and the Philippines, weaker states who, in the Chinese view, should remain mindful of their power. This perspective has also created problems with the United States whose Navy treats those waters under the same established norms as international waters, but who actions are often perceived as an affront to Chinese sovereignty (Kolton, 2017).

B. IS DETERRENCE EFFECTIVE?

There has been much debate on how to model the behavior of decision makers within the framework of deterrence theory as well as on the effectiveness of deterrence policies. A basic model for deterrence looks at the assumption of costs and risks in relation to the anticipated benefits, stating that if $C + R > B$, where C represents the costs, R the risks and B the benefits of taking a certain action, then the attacking force can be deterred. The attacker uses these estimates to determine whether it is worthwhile to attack, while the deterrer uses them to assess whether their deterrent strategy is adequate. The next step is to add the likelihood of the expected retaliation, adding a probability variable to the equation: $p(C + R) > (1-p)(B)$, where p denotes the probability of retaliation as estimated by the attacker. Both the attacker and deterrer may have different estimates of p, so if a deterrer would seek to raise this probability, then it must ensure the credibility, in the view of the opponent, that retaliation will follow (George & Smoke, 1974).

Others have used expected utility models to understand the issue from the positions of both the attacker and defender. This can be formalized in the equation $U_{a1}(p) + U_{a2}(1-p) > U_{a3}$, where U_{a1} is the utility of attacking if the defender fights back, U_{a2} is the utility of attacking if the defender does not fight back, and U_{a3} is the utility of not attacking, with p as the probability that the defender will fight. For the defender, the calculation would then be $U_{r1}(q) + U_{r2}(1-q) > U_{r3}$, with U_{r1} as the utility of resisting the attack if deterrence efforts fail, U_{r2} as the utility of resisting if the deterrence efforts succeed, U_{r3} as the utility of not resisting, and q being the probability that their deterrence efforts will fail (Huth & Russet, 1984).

In both of these models, the credibility of the threat from the deterrer plays a role. Deterrence can only be effective if the opponent believes that the threat of retaliation is real and that the defender has the will to act. Merely having a large stockpile of weapons or superior capabilities is not enough. In fact, it has been noted that states with superior capabilities most often do not initiate conflict; it is parties with inferior capabilities who tend to attack first (Russet, 1963). Often overall capabilities and strength are less important than the perceived ability to secure success in one's attack before retaliation can begin. (Gerson, 2009).

These simple models lack other factors, which must be considered to understand a country or leader's choice of actions on issues, such as trade, alliances, and local military balance (Huth & Russet, 1984). Furthermore, rational thinking based on objectively calculated outcomes is not necessarily applied, perception can prove more important than reality, and even a rational actor may make an irrational choice if there appears to be no good alternative. Deterrence is never guaranteed. The policy itself could have been ill conceived or an optimal policy could have been frustrated by an unknowable event (Jervis, 1989). Despite the imperfect application of deterrence theory in real scenarios, deterrence as a concept continues to play an important role in international relations and defense strategies.

C. ISSUES WITH CYBER DETERRENCE

As networking and computer-based systems have become ubiquitous in many areas of our lives, including for governments, these systems provide new opportunities to infiltrate and disrupt adversary operations and gather information. Weapons and strategies that could enforce deterrence in the past, such as conventional weapons, nuclear weapons, or sanctions, remain available to discourage unwanted actions against our interests in the virtual domain. But cyberspace also provides new ways to deter adversaries.

A body of literature frames issues related to cyber deterrence in the mold of nuclear deterrence (Libicki, 2016). Overall, there are far more differences than similarities. Unlike nuclear weapons, cyber munitions can be created with a large range of capabilities and to produce many potential results. Nuclear weapons are all efficient bombs. Cyber weapons can shut down an industrial control system, capture keystrokes, turn on or off power, increase the speed of an autonomous vehicle, or manipulate, erase, or create data. Furthermore, while indiscriminate death and destruction are results of deployment of nuclear weapons, cyber weapons can be engineered not to cause this level of physical damage. Therefore, many of their uses will not be considered to have crossed a red line for retaliation and thus the potential for destructive counterattack will not be a deterrent to the attack.

Cyber weapons differ from conventional and nuclear weapons in that damage assessment is difficult (Rowe, 2010). For example, if a cyber munition is intended to shut off power to a military installation and nothing is reported, it could be the target is concealing what happened or it could be that the weapon did not work. Furthermore, if it is observed that the power has indeed gone down, the weapon may have succeeded, but the power outage could also be the result of someone having tripped a breaker or routine maintenance. Therefore, as deterrence relies heavily on the credibility of the threat, a cyber weapon which might fail to achieve its intended aim or which could not be determined to have done so has a weakened deterrent effect against future attacks. Furthermore, as cyber weapons often exploit specific vulnerabilities, a demonstration of a

cyber weapon to prove its capability exposes the knowledge of those vulnerabilities and provides clues to patching it. The weapon then ceases to be effective as a deterrent.

Attribution provides another difference between cyber weapons and conventional or nuclear weapons. Were conventional or nuclear weapons to be delivered by aircraft, the source of the weapons would be known with high certainty from knowledge of the aircraft and its route. With cyber weapons, such certainty is not always possible. Many methods may need to be used for attribution, some of which can take extended time. Stealth and deceptive techniques are also often employed with such weapons, adding an extra layer of complexity that does not exist for nuclear weapons. Moreover, cyber weapons can be easily sold or donated, further complicating the question of attribution. The inability to reliably attribute a cyberattack can pose a problem for those who wish to deter them.

D. UNITED STATES POLICIES ON CYBER DETERRENCE

The United States has issued many strategy and policy documents about actions in cyberspace and protection of cyberspace covering the use of cyber weapons and the application of deterrence. Responsibility for cybersecurity policy falls under a large number of U.S. government and Department of Defense (DoD) agencies. However, we identify the main documents.

In February of 2003, recognizing officially that cyberspace is integral to the economy and to national-security interests, the White House published The National Strategy to Secure Cyberspace. The document outlined a framework for securing cyberspace from actors on a national, state, and local level. The three strategic objectives outlined were to: 1) “prevent cyberattacks against America’s critical infrastructures; 2) reduce national vulnerability to cyberattacks; and 3) minimize damage and recovery time from cyberattacks that do occur” (The White House, 2003, p. viii).

The International Strategy for Cyberspace focused not just on domestic issues but also incorporated proposals for how to achieve the United States’ desired outcomes in partnership with the international community (The White House, 2011). It also directly discusses the issue of deterrence by denial and punishment:

> The United States will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits…When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country…We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. (pp. 13-14)

This was the first official U.S. document to indicate an explicit policy of deterrence in cyberspace.

The 2015 U.S. DoD Cyber Strategy aimed to "guide the development of the DoD's cyber forces and strengthen our cyber defense and deterrence posture" (Department of Defense, 2015, sec. Foreword). It outlined broad objectives for DoD cybersecurity operations in partnership with other domestic agencies and international partners. The three categories of efforts indicated as essential to contributing to improving the strength of U.S. networks and defensive capabilities are response, denial and resilience.

The 2015 National Security Strategy identified cyberspace as a major focus of national security. It referenced goals including the creation of "long-standing norms of international behavior" to combat the range of cybersecurity threats, and placed it first in the list of shared spaces to which access should be assured (The White House, 2015, p. 13). An updated National Security Strategy from 2017 also addressed issues of cybersecurity and prevention of cyberattacks from adversaries (The White House, 2017). Protection of American assets that are vulnerable to cyberattack, including communication channels, the electrical grid, and federal networks, are a key part of the strategy, with an emphasis on deterrence by denial.

The Defense Science Board Task Force on Cyber Deterrence issued a report detailing its recommendations for strengthening cyber deterrence and outlining major cyber threats, including those from state and non-state actors (Defense Science Board, 2017). The report noted that the threat of cyberattacks was increasing faster than vulnerabilities could be identified and patched, and therefore, that deterrence must play a major role in the protection of the U.S. and its allies in this sphere. The importance of

resiliency for critical infrastructure and military systems, along with the need to adjust deterrence efforts to particular adversary tactics and to improve attribution capabilities were also addressed.

The 2018 revision of Joint Publication 3-12 from the Chairman of the Joint Chiefs of Staff provided updated guidance to the United States Armed Forces on cyberspace operations (Chairman of the Joint Chiefs of Staff, 2018). In addition to detailing issues relating to authority and integration of cyber operations with the traditional domains (land, sea, and air), the document outlined expectations for planning, executing and assessing these operations. It also addressed areas of particular consideration, such as overlapping or shared networks, interconnectivity and the potential impact of retaliation on regular military operations.

III. CAPABILITIES AND STRATEGIES OF THE UNITED STATES AND MAJOR ADVERSARIES

A. RUSSIA

Russia views itself as subject to constant threats, both external and internal, attempting to erode the power of the Russian State and its leaders. They are, therefore, in the midst of an ongoing campaign to maintain power and fight against these adversaries. A 2018 report from the Estonian Intelligence Service indicates that "Russia believes that the state is forced to wage a hidden political struggle against the West" (Estonian Intelligence Service, 2018, p. 46). Disinformation campaigns and electronic warfare along with psychological operations have long been employed by Russia to combat this threat. Cyber operations are an added subset of the information operations that have been an integral part of their traditional strategies going back to the Soviet era (Connell & Vogler, 2017). As such, Russia sees no major distinction between peacetime and wartime, since actions must be taken on a consistent basis in order to maintain the power balance and prevent adversarial gains.

Along these lines, Russian attempts to influence U.S. domestic politics by sowing misinformation and fomenting unrest have been seen in several cases. In addition to hacking and gathering documents and other information, the Russians were also accused of creating fake internet personas and spreading inflammatory articles and tweets in support of radical and divisive causes in the U.S. in 2016. In July 2018, twelve Russian intelligence agents were indicted for their involvement in hacking the Democratic National Committee (DNC) network and Clinton presidential campaign servers (Mazzetti & Benner, 2018). Another example of operations of this type is Russian interference in Greece and Macedonia in an attempt to keep Macedonia from joining NATO and aligning itself with the West. In June 2017, leaked confidential documents from the Macedonian intelligence services revealed Russian strategic interference in their internal affairs dating back to 2008 (Harding, Belford, & Cvetkovska, 2017).

Another tactic attributed to Moscow is the use of proxy agents to conduct cyber operations on their behalf, a strategy that allows their desired ends to be achieved while

providing enough obfuscation to avoid accountability. In April and May 2007, Estonia suffered major distributed denial-of-service attacks. While the attacks were never definitely tied to the Russian government, evidence showed that they were perpetrated by Russia actors (Davis, 2007). Recently, several proxy groups have been reliably linked to the Russian government; however, use of hacktivists and other pro-government operators has proven to be a successful way to maintain a certain level of deniability, whether or not it is plausible.

The Russians have also used offensive cyber operations as part of larger campaigns. In 2008, Georgia found itself on the receiving end of a denial-of-service and website defacement campaign in the run-up to a military conflict with Russia (Markoff, 2008). In December 2015, electrical power went out for almost 250,000 Ukrainians in a massive attack on several power supply companies. Malicious firmware updates had also been created to compromise the Supervisory Control and Data Acquisition (SCADA) systems of these power companies, which took months to repair even after the power was finally turned back on (Zetter, 2016). The following year, the power grid was again taken offline, with signs pointing to Russian involvement (Greenberg, 2017).

At present, deterrence efforts against Russian actions in cyberspace do not appear to be succeeding. In June of 2013, the U.S. and Russia agreed to cooperate on matters related to malicious actors or malware use inside their territories in an effort to combat malicious cyber activity (The White House, 2013). Such an agreement supported collaboration and information sharing on joint threats while also attempting to hold the Russian government responsible for actions originating in their country. However, as Russia has continued to launch increasingly damaging cyberattacks against the U.S. and allied nations since this agreement, the secondary aim has not been achieved. Russia continues to be undeterred in their denial-of-service attacks against the Ukraine, and as the indictment of the Russians for the 2016 U.S. elections hacking shows, their efforts against the U.S. have intensified as well (Mazzetti & Benner, 2018).

B. CHINA

The Chinese view on information space is that cybersecurity not only involves the protection of data and networks from malicious actors but also includes the defense of and influence over what content is available to citizens. The disconnect between Chinese and Western understanding of terms and extent of state control in cyberspace has often prevented progress on bilateral agreements, especially in regard to cyber espionage and theft of intellectual property (Giles & Hagestadt, 2013).

The Chinese have strategically used international discussions and transnational forums as well as bilateral and other international agreements to promote the understanding of their dominance and overall prowess in the realm of cyber warfare (Sowers, 2018). By signing on to major agreements to restrict use of cyber warfare capabilities, the Chinese have ensured that they are seen as possessing these capabilities without having to overtly display them.

The Chinese have, however, used their cyber capabilities against adversaries who are not in a position to retaliate strongly. For instance, the Philippines government has accused Chinese hackers of instrumenting distributed denial-of-service attacks against several government websites in the aftermath of a Permanent Court of Arbitration ruling passed down in favor of the Philippines on 12 July 2016, about disputed claims over territory in the South China Sea (Cimpanu, 2016). Additionally, a Chinese group was accused of organizing an attack against Vietnamese airport infrastructure and defacing national airline websites at the end of July 2016 in response to Vietnamese support of the Philippine's position (Clark, 2017).

While the Chinese do not seem to be deterred in their actions against weaker states, they have tended to avoid attacks against stronger powers in favor of infiltration of networks and theft of intellectual property. In 2015, an agreement was made between Beijing and Washington to cooperate on a number of key issues, including theft and economic cyber threats. The agreement omitted mention of other types of malicious cyber activity such as infiltrating government databases or military installations, despite the fact that it was reached only months after the hack of the Office of Personnel

Management (OPM) which was later attributed to China where personal data of over 20 million government employees and contractors was stolen (Davis, 2015). As many of the Chinese actions against the U.S. are cyber espionage rather than attacks, such as the OPM hack and thefts of plans for military equipment (Cooper, 2018), they often fall outside of scope of many DoD-centered deterrence efforts. Nonetheless, Chinese economic espionage exploits can hurt national security interests and directed efforts are required to prevent and discourage them.

C. NORTH KOREA

As North Korea does not maintain an advantage with its conventional military forces, asymmetric operations are an important part of its strategy. Investments in cyber capabilities, much like earlier ones in nuclear weapons and ballistic missiles, offer an ability to counter conventional attacks by causing maximum damage from a distance. Furthermore, unlike nuclear or missile attacks, many cyberattacks do not rise to the level of armed attack, and therefore do not invite retaliation. This makes them ideal tools for interfering with adversaries without worry of provoking an escalated response.

One example of this type of action is the attack on Sony Entertainment Pictures in 2014 (Sanger, Kirkpatrick, & Perlroth, 2017). The WannaCry ransomware attack from 2017, which caused damage to many public and private entities, including hospitals and the United Kingdom National Health Service, has also been attributed to North Korea (BBC, 2017). There have also been many attacks by North Korea against South Korea, such as the use of wiper malware against three banks and two broadcast companies in 2013, during joint U.S. and South Korean military exercises, and exfiltration of military action plans and other documents from a South Korean military data center (Sanger, et. al, 2017; Kim, 2017).

In the North Korean view, “securing and disrupting systems, a function of cyber warfare, is thought of as a part of a larger information warfare strategy” (Jun, LaFoy, & Sohn, 2015, p. 31). Much like techniques of electronic warfare, which serve to inhibit proper functioning of munitions and information channels, such as jamming or satellite signal interference, cyberattacks can be used to cripple the weapons and communications

systems of an opponent. By investing in all aspects of information warfare, including cyber capabilities, North Korea targets adversaries' vulnerabilities during peacetime and seeks to create maximum cost during wartime, achieving their goal of disruption and influence despite resource constraints.

The North Koreans have been quite active in their cyber actions against both the U.S. and South Korea, as well as causing more damage worldwide. The response to their actions has mostly consisted of nations publicly calling them out as the perpetrator of the attacks, which has done little to curb the behavior. Other attacks attributed to North Korea, such as the theft of $81 million from Bangladesh's account with the New York Federal Reserve Bank in 2016 and gaming exploits in South Korea appear to be aimed at generating foreign currency for the regime (Jun, et. al., 2015). Despite being one of the most heavily sanctioned and impoverished nations, North Korea does not seem to be deterred in their cyber exploits, much as they have not been with nuclear weapons development.

D. IRAN

As with other states that lack the ability to match their adversaries in the conventional weapons arena, Iran has looked to bolster its strength through other means, including through nuclear weapons and cyberattack capabilities. On several occasions, "Iran has demonstrated how militarily weaker countries can use offensive cyber operations to contend with more advanced adversaries" (Anderson & Sadjadpour, 2018, p. 6). In 2013, it was announced that Iranian hackers were inside the unclassified network of the U.S. Navy for over four months before being discovered (Gorman & Barnes, 2014). Additionally, in March 2016, a Justice Department indictment was unsealed against seven Iranian nationals suspected to be working for the Iranian government who had perpetrated several denial-of-service attacks against major U.S. banks from 2011 to 2013, one of whom had also managed to gain access to the SCADA system controlling an upstate New York dam (Justice Department, 2016).

In addition to network infiltration and denial-of-service attacks, Iran has also proven that its cyber capabilities have been evolving. The Shamoon attack against the

Saudi oil company Aramaco in August 2012 was attributed to Iran by security researchers from several countries (Perlroth, 2012). This attack included an element that had been seen in an earlier attack perpetrated against Iran, indicating that the Iranians were able to incorporate information learned from that incident into their own cyber inventory (Zetter, 2015). The same malware was then used by Iran in an attack against the Qatari RasGas company later the same month (Zetter, 2012). These incidents show that Iran has been able to leverage their capabilities in cyberspace to move beyond merely causing a nuisance to their adversaries, having proven that they can cause harm and destruction.

The international community has managed to deter Iran to some extent in their aims to develop nuclear weapons through sanctions and inspections. However, with the withdrawal of the U.S. from the nuclear deal earlier this year, there has been speculation from the intelligence community that Iran will increase their cyber activity, particularly against the U.S., in retaliation for what they feel is unfair treatment (Landler, 2018; Riechman, 2018). Up to this point, Iran has tested their capabilities against various other nations and there is little evidence that anything other than their own knowledge has deterred them from going farther than they have already.

E. UNITED STATES

The United States undertakes cyber operations from both the offensive and defensive perspectives and uses its cyber capabilities alongside more traditional military operations. Seeking to prevent unauthorized access to its networks and critical infrastructure, over the last several years, the government has adopted a series of policies and programs aimed at improving defensive capabilities of the DoD and other federal agencies. The U.S. has also made a push to train offensive cyber operators, working to increase its arsenal of cyber weapons and create a force that is competent to deploy them.

On the offensive front, the U.S. has conducted several major operations. One of the earliest was the provision of faulty chip design software to the Soviet Union that resulted in a massive explosion of the Trans-Siberian gas pipeline in 1982 (Safire, 2004). The U.S., along with Israel, is attributed with creating and deploying the Stuxnet malware

that caused the failure of centrifuges at the Natanz nuclear facility in Iran (Nakashima and Warrick, 2012). The U.S. has also used its cyber capabilities to manipulate content on websites and disable internet infrastructures operated by terrorist groups such as Al Qaeda and ISIS (Cox, 2018; Hudson, 2012).

While the U.S. has not shied away from offensive actions, most U.S. Cyber Command efforts have been concentrated on defensive programs. However, a recent change in policy has granted the command more authority to conduct offensive operations (Sanger, 2018). This may be a reaction to the perceived failure of other methods of deterring adversaries. The U.S. has come under attack domestically for their inability to stop major cyberattacks, including the 2016 elections hacking. Some have noted that while the U.S. has an interest in deterring others from conducting cyber operations, they were themselves deterred from taking action as soon as these hacks were attributed to Russia for fear of escalation or perhaps superior Russian capabilities (Healy, 2018).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CYBER ACTIONS FOR DETERRENCE

A. INTRODUCTION

Just as with other types of weaponry and forms of conflict, there are many ways to make deterrence work in cyberspace, since different methods can be more or less effective in different circumstances. The below outlines several actions that can be taken to deter adversaries from using their cyber weapons capabilities. These options can be implemented alone or integrated as part of a comprehensive deterrence framework.

B. STOCKPILING

For conventional and nuclear weapons, one way countries try to achieve deterrence is through the build-up of their own arsenals of munitions. This increase in weaponry can occur in the presence or absence of agreed limitations. Without restrictions on arms development, countries can enter an arms race; otherwise, build-up continues until an agreed level has been reached. Both courses of action are claimed to result in deterring the opponent from using their weapons (Figure 1).

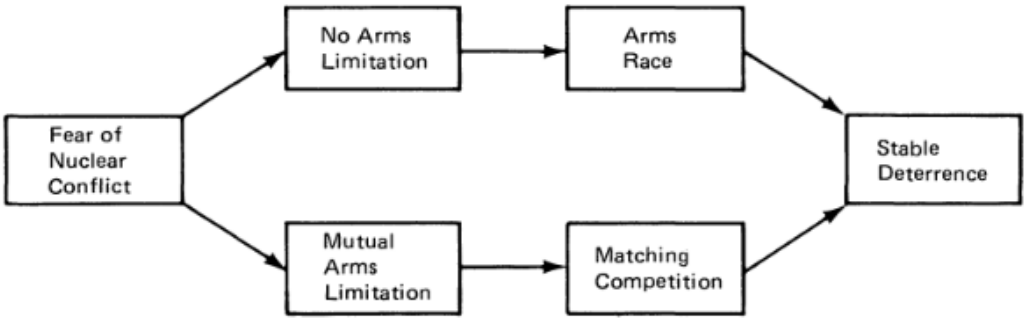

Figure 1. Arms Competition and Deterrence. Source: Kugler, Organski, and Fox (1980).

The deterrent effect comes not from the deployment of these arms but from their stockpiling. As indicated earlier, deterrence requires a credible threat of serious retaliation. If a nation can show that they possess weapons capable of enacting that threat, then credibility will have been achieved.

With cyber weapons however, the case for building a stockpile might not be straightforward. A nation can claim to possess cyber weapons and to be actively working on increasing their arsenal. However, such an accumulation would be less visible than with other kinds of weapons. One could claim to have a capability and threaten opponents with it, but until the weapon has been used, no one can know for certain whether it exists or is effective. Therefore, use of a cyber weapon's capability is important to the credibility of its threat. But there is a tradeoff because use of a weapon gives away many of its secrets and makes reuse less likely to be effective.

C. DECEPTION

Credibility with cyber weapons can be manipulated by using deception, as perception is often more important than reality. After the attribution of the 2016 election hacking to Russia, some in the U.S. suggested retaliation with cyber weapons but this ultimately did not take place. One reason put forth was that the U.S. feared their actions would be seen as escalatory, but others believed the Russians would end up winning such a cyber battle (Healy, 2018). Whether the Russians had superior capabilities or not does not matter if the impression that they did prevented the U.S. from taking any overt cyber action against them.

Several deceptive techniques can be used to create an impression of cyber weapons capabilities. For example, leaking "confidential" documents in reference to capabilities that have not actually been achieved can create the impression that they are ready for use. Hinting at missions that have been achieved in press conferences and interviews is another way to promote one's capabilities without using a weapon or performing a demonstration. Alternatively, a false capability could be simulated in a controlled setting where the results shown are not actually those of the cyber weapon being tested. Such an event requires some degree of secrecy.

Deception can also compromise opponents in other ways. For example, theft of intellectual property and trade secrets by China from the government and military makes it possible to plant false documents where a network infiltrator would expect the real documents to be. These documents could give designs that will ultimately not work or

could have software or hardware backdoors (clandestine access portals) in them. Strategically placing these documents on known networks of interest could slow down or compromise an adversary's advancement efforts and could provide a way to shut down malicious systems later if desired. An adversary who is the victim of these efforts might be deterred from stealing such documents in future if they are known to be untrustworthy or to compromise their own network security.

D. INDICTMENTS OF INDIVIDUALS

Cyberattacks usually violate criminal laws. Over the years, the U.S. has issued detailed indictments for several perpetrators of attacks against the government and financial institutions done on behalf of nation states including Iran and Russia. The U.S. has also indicted Chinese nationals, both in 2014 and 2017, for cases of hacking related to economic espionage (Justice Department, 2014 & 2017). No individuals named in these indictments have been extradited, nor has any action been taken to bring them in by their governments. However, a Chinese hacker was arrested in August 2017 in Los Angeles on charges of using the same malware as the perpetrators of the OPM hack two years before (Barrett, 2017).

With regard to the Russian indictment, "some experts said that the granular detail in the indictment was a warning to groups who might be eyeing future attacks" (Mazzetti & Benner, 2018). However, as these indictments have yet to produce any extraditions or prosecutions, it is hard to see how effective this warning would be. When perpetrators of cyberattacks are acting on behalf of their governments, it seems natural that they would be afforded protections at home. While an indicted individual might risk arrest or extradition while traveling to a country that has an agreement with the U.S., many of these actors are not at liberty to choose their involvement or travel freely. Therefore, indictments serve only as a weak deterrent mechanism.

E. SANCTIONS

Sanctions have been an effective deterrent in some instances. One example of a fairly successful case is the Iraqi dismantling of its chemical weapons program in the mid-1990s (Central Intelligence Agency, 2007). On the other hand, sanctions against

North Korea to deter its development of nuclear weapons have proven to be a failure. It is possible to impose sanctions on a nation after their use of cyber weapons or sponsorship of cyberattacks. However, many nations that have sponsored cyberattacks, including Russia, North Korea and Iran, are already subject to sanctions for other reasons. Additionally, sanctions are usually targeted against certain industries or products, but it would be infeasible to sanction the purchase of computer equipment or software. Agreeing on a set of norms would help ensure the imposition of sanctions was not seen as arbitrary or overly harsh.

F. INTERNATIONAL AGREEMENTS

A set of international norms for acceptable actions in cyberspace can contribute to deterrence. As with other weapons, such as chemical or biological weapons or cluster munitions, states can agree, at minimum, on which types of cyber weapons are acceptable for use and which should be banned. Since different cyber weapons can achieve the same end, a good system should categorize them by the expected results.

Some preliminary work toward this end has been the United Nations (UN) Group of Governmental Experts reports from 2013 and 2015, which concluded that existing international law, including the UN Charter, applies to cyberspace and recommended the prohibition of state-sponsored attacks on critical infrastructure. However, the latest round of talks in 2017 failed to produce a consensus (Korzak, 2017). NATO has also published the Tallinn Manuals that outline the applicability of international law to cyber warfare and peacetime operations (Schmitt, 2015; Schmitt & Vihul, 2017). These publications seek to create a common understanding of permissible actions in cyberspace; however, none rises to the level of a legally binding treaty on cyber munitions. Therefore, more work is required to achieve this end.

If not all states adhere to these norms or standards, their effect will be more limited. Strong states that subscribe to the concept of red deterrence may feel the rules apply only to others, and without a common understanding, it is hard to foster an environment of mutual trust. As with other international agreements, there may be those who chose not to accede or who sign but later withdraw, as North Korea did with the

Nuclear Non-Proliferation Treaty in 2003. But such treaties can have a deterrent power on many others, and efforts should be made to persuade those countries who pose the greatest risk to adhere.

G. NON-CYBER RETALIATION

The threatened response to a cyberattack could include the use of conventional or nuclear weapons. They should not be the first choice, but such retaliation methods should be considered in cases of very serious attacks. This would most likely be seen as escalatory due to the overt destructiveness of such weapons, but such a response would ensure the adversary knows their actions are unacceptable and increases the weight of their decision to continue them. There is a risk that the attacker may counter-respond with conventional force and continue the escalation, however.

H. IMPROVING DEFENSES

Deterrence by denial can be effective when conducting an attack can be clearly shown to be costly compared to the likely benefit. In the case of cyberspace, increasing one's defenses is unlikely to deter the adversary from trying at all, since the potential for a major gain from such efforts does exist. However, there are labor costs and time constraints associated with attempting to infiltrate a network or reverse engineer a SCADA protocol for a water or power system. As the tactical benefits do not always compensate for this cost, an attacker may be deterred. While there have been a large number of successful cyberattacks against U.S. businesses, including Equifax, Anthem, Target and Chase Bank, there have been substantially fewer against military and DoD entities (Center for Strategic and International Studies, n.d.). While it is true that many cyberattacks against private sector entities are perpetrated by criminals interested in monetary gains, nation-state sponsored actors have also been implicated in this type of attack (Justice Department, 2014). This evidence could suggest that since the barrier to success is higher for government targets, certain attackers have been deterred.

Note that making one's networks difficult to infiltrate and protecting one's systems provides the additional benefit of keeping information and structures safe. Furthermore, intercepting malware from attacks can help to understand the adversary's

aims and capabilities. Honeypots and honeynets can also serve to keep the adversary engaged in ineffective activities giving the defender time to discover and learn from the breach before any damage to the real systems is done. Thus, cyber defense is well justified even though it does not always deter.

I. AUTOMATED COUNTERATTACK

Deterrence could also be achieved through the threat of automated counterattack. For example, a weapon could be created so that if a defender's sites are attacked or intellectual property or other sensitive information is exfiltrated, it would automatically insert malware, such as a virus or backdoor, or other modifications into the compromised documents. The malware could be designed to harm the original attacker's systems or warn them to stay out. Modifications to exfiltrated data could also be used to gain access to the attacker's systems. An adversary who knows of a defender with such capabilities could be deterred from attacking. However, there are potential dangers with such a strategy, as an innocent party, whose systems were used without their knowledge to launch the attack, could end up the victim of such retaliation.

J. MOUNTING OFFENSIVE CYBER ACTIONS

Offensive cyber operations may serve as deterrents by forcing adversaries to use their resources for defensive purposes, thereby leaving fewer resources available for conducting offensive operations. Secondly, such actions can provide demonstrations of capabilities that can in turn increase deterrence credibility. Recently, there has been some support for this type of activity within the U.S. government (Sanger, 2018).

These cyber operations can have narrow aims, as with Stuxnet or the Trans-Siberian Pipeline operations (Nakashima and Warrick, 2012; Safire, 2004). Offensive operations can be run to dismantle or degrade the capabilities of certain known actors and groups. Even though the target of these operations may be limited, demonstrations of the capabilities used in the campaign could deter states other than those who were attacked.

Deterrence effects are enhanced by creating more reliable cyber weapons and laying the groundwork for their use. With a better and more dependable arsenal, it will be

easier to make the decision to use those weapons should the situation arise, and these weapons should provide more deterrence effects. Part of creating a credible cyber threat requires convincing adversaries than the weapons will do what they are expected to do, and this convincing is easiest when it is true.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND SUGGESTIONS FOR FUTURE RESEARCH

A. CONCLUSIONS

Cyber deterrence is becoming more possible. A past reason for the inability to respond swiftly in the case of a cyberattack was the difficulty of determining definitively who perpetrated the attack. Given the advances in this field, attribution less often hinders prompt reaction in many cases, which can permit rapid targeted retaliation in the wake of an assault (Rid & Buchanan, 2015). Publicly announcing that a cyberattack has been found to be the result of state-sponsored activity alerts the offenders and others to a state's attribution capabilities and can serve to prevent a response from being seen as arbitrary or escalatory. This allows a state to use a wider variety of capabilities to respond to cyberattacks, which can aid in deterring future attacks.

States can use cyber or non-cyber retaliation, including automated counterattack capabilities, when they are victims of a cyberattack. Developing such automated response capabilities can add credibility to the threat of retaliation as successful use of these weapons demonstrates the will and ability to counterattack. Furthermore, if these weapons are only deployed after an offensive attack and their effects are not overly destructive, they would potentially be justifiable to the international community. However, as mentioned in Chapter IV, an innocent party could fall victim to an automated response.

Cyber weapons whose capabilities can be convincingly exhibited can have a stronger deterrent effect than those that cannot be. Just as militaries stage demonstrations to show off new equipment and display novel weapons capabilities, the United States can do the same with its cyber weapons. Such a performance could provide a way to show what damage they can cause without giving away the secret of the cyber weapon, since only the effects, not the code that produced them, would be seen by outsiders. An example of a similar type of experiment was operation "Aurora" conducted by the Department of Homeland Security in 2007, which demonstrated the exploitation of a known vulnerability to destroy a power generator at Idaho National Labs (Meserve,

2007). While this demonstration was intended to convince the energy industry to strengthen their security. Similar techniques aimed at showing cyber weapons capabilities can serve to bolster credibility, an essential component of deterrence. Alongside genuine displays, deception can be used to foster the perception of better weapons if required; however, it should be used sparingly because deception, if discovered, will quickly invalidate deterrence.

It may be true that capabilities can be most credibly demonstrated through offensive cyber operations; however, there are also drawbacks. While controlled displays allow more secrets of the weapons to be kept, their use in offensive operations risks giving that knowledge to the adversary who can use digital forensics to analyze them in detail. Furthermore, there are many legal considerations that would necessarily factor into any offensive action, while a staged demonstration could proceed without such worries.

Improvements in defenses should also be undertaken for deterrence. Here too, deception could be incorporated in the U.S. deterrence strategy. Honeypots and honeynets can consume the resources and time of an adversary and provide valuable clues to their methods of operation. As one of the major complaints for the U.S. at present is exfiltration of intellectual property and technical plans, planting compromised files or embedding backdoors in bait documents intended for exfiltration can provide an opportunity to neutralize the effects of such theft and can potentially provide access to adversary networks. If repeated attempts at exfiltration prove fruitless and expose their own networks, adversaries may choose not to continue them. The U.S. should also develop better tools to detect and alert network-security operators to breaches and malicious activity and keep critical information and networks isolated from the Internet to the greatest extent possible. Making infiltration of a network harder and increasing an adversary's likelihood of getting caught provide an increased deterrent effect.

While the international community has considered issues of security in cyberspace, more work is needed to seek agreement on acceptable cyber actions and to formulate a unified response to certain actions. Sanctions and naming and shaming work better if a group of nations agrees on them. By discussing the critical issues and designating certain cyber actions as unacceptable, nations can operate from an agreed

understanding. They then can work together to hold rogue states to account through sanctions, indictments, and other diplomatic means, which should provide some deterrence against cyberattacks. The United States should lead the effort to continue these discussions to bolster the effectiveness of these tools as part of its deterrence efforts.

Creating a large stockpile of cyber weapons appears to be unlikely to have much deterrent effect, unless most weapons could be credibly demonstrated, and few cyberattacks would be serious enough in their effects to justify use of such an arsenal. Therefore, efforts should be spent on creating only those weapons that would be the most useful, such as automated counterattack capabilities and strategic weapons with narrow aims, rather than building a large stash of weapons with highly destructive capabilities.

States are aware that retaliation for a cyberattack could include the use of conventional weapons. However, such a response has yet to be seen from the United States. Therefore, the threat of conventional retaliation by the U.S. does not provide much cyber-deterrence as it may seem that the U.S. lacks the will to respond in a way that would seem escalatory. But international law, which permits the use of force only in self-defense against armed attacks, is a consideration for such action as well (United Nations, 1945). Nevertheless, as the United States faces the continued threat of cyberattack from several adversaries, it could work with its allies to take visible collective action against those that would seek to undermine its interests. Strong retaliation should be forthcoming when provoked and can be justified if it can be shown that the accumulation of the damage from a number of small attacks does indeed rise to a level that action in self-defense is required (Lin, 2010).

B. SUGGESTIONS FOR FUTURE RESEARCH

Many cyberattacks from China, Iran, and North Korea, and to some extent Russia, have more in common with crime and espionage than with combat. Looking into ways to fight state-sponsored crime can provide additional tools to deter these types of actions. Past cases of criminality can be looked at to determine what has been effective in curbing it and to what extent, and recommendations could be made where crossover successes of these strategies can be envisioned. For example, profiling cyber criminals and making

note of their signatures or maintaining repositories of malicious code indexed by country of origin could potentially be helpful.

Deterrence of other forms of cyber threats such as misinformation campaigns should be considered as well. Many of the most harmful cyber threats that we are seeing today are extended and complex propaganda campaigns aimed at undermining state authority and causing civic unrest. Such strategies are employed by both Russia and North Korea as part of their military doctrines. Research should be conducted to find methods to help government and private sector entities monitor news stories and social-media posts associated with these campaigns, along with ways to help citizens inoculate themselves against these efforts.

A distinction between cyber espionage, cybercrime, and cyberattack can hinder the U.S. government's ability to comprehensively respond to the full cyber threat. Network infiltration can result in information being gleaned for espionage purposes, theft of intellectual property or access to critical infrastructure, so deterrence planning should use a broad strategy. This includes prevention of attacks on private sector entities that could compromise national security. When private-sector issues create public risk, a government must take action and it should be strong. Work to improve cooperation and information sharing between the many government agencies dealing with cyberattacks can help to provide a more comprehensive deterrence strategy.

LIST OF REFERENCES

Anderson, C., & Sadjadpour, K. (2018). *Iran's cyber threat: Espionage, sabotage and revenge*. Washington, DC: Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

Barrett, D. (2017, August 24). Chinese national arrested for allegedly using malware linked to OPM hack. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html?utm_term=.0006ca3f9cf6

BBC. (2017, December 19). Cyber-attack: US and UK blame North Korea for WannaCry. Retrieved from https://www.bbc.com/news/world-us-canada-42407488

Center for Strategic and International Studies. (n.d.). Significant cyber incidents. Retrieved from https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Central Intelligence Agency. (2007, April 23). Iraq's chemical warfare program. Retrieved from https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/chap5.html

Cimpanu, C. (2016, July 18). Philippines government websites hit by massive DDoS attacks, China suspected. Retrieved from https://news.softpedia.com/news/philippines-government-websites-hit-by-massive-ddos-attacks-china-suspected-506412.shtml

Clark, H. (2017, December 6). The alleged Chinese hacking at Vietnam's airports shows that the South China Sea battle isn't just in the water. *Huffpost*. Retrieved from https://www.huffingtonpost.com/helen-clark1/china-hack-vietnam-south-china-sea_b_11357330.html

Connell, M., & Vogler, S. (2017). *Russia's approach to cyber warfare*. Arlington, VA: CNA. Retrieved from https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Cooper, H. (2018, June 8). Chinese hackers steal unclassified data from Navy contractor. *The New York Times*. Retrieved from https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html

Cox, J. (2018, August 1). How US military hackers prepared to hack the Islamic State. Retrieved from https://motherboard.vice.com/en_us/article/ne5d5g/how-us-military-cybercom-hackers-hacked-islamic-state-documents

Davis, J. (2007, August 21). Hackers take down the most wired country in Europe. *Wired*. Retrieved from https://www.wired.com/2007/08/ff-estonia/

Davis, J. H. (2015, July 9). Hacking of government computers exposed 21.5 million people. *The New York Times*. Retrieved from https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

Estonian Foreign Intelligence Service. (2018). *International Security and Estonia*. Tallinn, Estonia: Estonian Foreign Intelligence Service. Retrieved from https://assets.documentcloud.org/documents/4378262/Estonian-Foreign-Intelligence-Service.pdf

Gerson, M. S. (2009). Conventional deterrence in the second nuclear age. *Parameters, 39*(3), 32-48.

George, A. L., & Smoke, R. (1974). *Deterrence in American foreign policy: Theory and practice*. New York: Columbia University Press.

Giles, K., & Hagestadt, W., II. (2013). Divided by a common language: Cyber definitions in Chinese, Russian, and English. In *5th International Conference on Cyber Conflict*. Retrieved from https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf

Gorman, S., & Barnes, J. (2014, February 18). Iranian hacking to test NSA nominee Michael Rogers. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/iranian-hacking-to-test-nsa-nominee-michael-rogers-1392694544?tesla=y

Greenberg, A. (2017, June 20). How an entire nation became Russia's test lab for cyberwar. *Wired*. Retrieved from https://www.wired.com/story/russian-hackers-attack-ukraine/

Harding, L., Belford, A., & Cvetkovska, S. (2017, June 4). Russia actively stoking discord in Macedonia since 2008, intel files say. *The Guardian*. Retrieved from https://www.theguardian.com/world/2017/jun/04/russia-actively-stoking-discord-in-macedonia-since-2008-intel-files-say-leak-kremlin-balkan-nato-west-influence

Healy, J. (2018, June 11). Not the cyber deterrence the United States wants. Retrieved from https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants

Hudson, J. (2012, May 24). U.S. counter-terrorism hackers fight Al Qaeda one prank at a time. Retrieved from https://www.theatlantic.com/international/archive/2012/05/us-counter-terrorism-hackers-fight-al-qaeda-one-prank-time/327722/

Huth, P., & Russet, B. (1984). What makes deterrence work? Cases from 1900 to 1980. *World Politics, 36*(4), 496-526.

Jervis, R. (1989). Rational deterrence: Theory and evidence. *World Politics, 41*(2), 183-207.

Jun, J., LaFoy, S., & Sohn, E. (2015). *North Korea's cyber operations: Strategy and responses*. New York, NY: Center for Strategic and International Studies. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf

Kim, C. (2017, October 10). North Korea hackers stole South Korea-U.S. military plans to wipe out North Korea leadership: Lawmaker. *Reuters*. Retrieved from https://www.reuters.com/article/us-northkorea-cybercrime-southkorea/north-korea-hackers-stole-south-korea-u-s-military-plans-to-wipe-out-north-korea-leadership-lawmaker-idUSKBN1CF1WT

Kolton, M. (2017). China's pursuit of cyber sovereignty and its views on cyber deterrence. *Cyber Defense Review, 2*(1), 119-154.

Korzak, E. (2017, August 01). UN GGE on cybersecurity: The end of an era? Retrieved from https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

Kugler, J., Organski, A. F., & Fox, D. J. (1980). Deterrence and the arms race: The impotence of power. *International Security, 4*(4), 105-138.

Kugler, T., Kausel, E. E., & Kocher, M. G. (2012). Are groups more rational than individuals? A review of interactive decision making in groups. *CESifo Working Paper Series, CESifo Group Munich, 3*(4), 471-482. Retrieved from https://EconPapers.repec.org/RePEc:ces:ceswps:_3701

Landler, M. (2018, May 8). Trump abandons Iran nuclear deal he long scorned. *The New York Times*. Retrieved from https://www.nytimes.com/2018/05/08/world/middleeast/trump-iran-nuclear-deal.html

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND.

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

Lin, H. S. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law & Policy, 4*(63), 63-86.

Markoff, J. (2008, August 12). Before the gunfire, cyberattacks. Retrieved from https://www.nytimes.com/2008/08/13/technology/13cyber.html

Mazzetti, M., & Benner, K. (2018, July 13). 12 Russian agents indicted in Mueller investigation. *The New York Times*. Retrieved from https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html

Meserve, J. (2007, September 26). Sources: Staged cyber attack reveals vulnerability in power grid. Retrieved from http://www.cnn.com/2007/US/09/26/power.at.risk/

Nakashima, E., & J Warrick. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.0b5c2ac589d6

Perlroth, N. (2012, October 23). In cyberattack on Saudi firm, U.S. sees Iran firing back. *The New York Times*. Retrieved from https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Rid, T, and Buchanan, B. (2015) Attributing Cyber Attacks, Journal of Strategic Studies, 38:1-2, 4-37

Riechman, D. (2018, August 8). US braces for possible cyberattacks after Iran sanctions. *The Military Times*. Retrieved from https://www.militarytimes.com/flashpoints/2018/08/08/us-braces-for-possible-cyber-attacks-after-iran-sanctions/

Rowe, N. C. (2010). The ethics of cyberweapons in warfare. *International Journal of Technoethics, 1*(1), 20-31.

Russet, B. M. (1963). The calculus of deterrence. *Journal of Conflict Resolution, 7*(2), 97-109.

Safire, W. (2004, February 2). The farewell dossier. *The New York Times*. Retrieved from https://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html

Sanger, D., Kirkpatrick, D., & Perlroth, N. (2017, October 15). The world once laughed at North Korean cyberpower. No more. *The New York Times*. Retrieved from https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

Sanger, D. E. (2018, June 17). Pentagon puts cyberwarriors on the offensive, increasing the risk of conflict. *The New York Times*. Retrieved from https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html

Schmitt, M. N. (2015). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press.

Schmitt, M. N., & Vihul, L. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press.

Snyder, G. H. (1959). *Deterrence by denial and punishment*. Princeton, NJ: Princeton University.

Sowers, M. (2018, February 21). How Beijing's cyber security engagement incorporates the three warfares. Retrieved from https://www.internationalaffairs.org.au/australianoutlook/china-three-warfares-in-cybersecurity/

United States Chairmen of the Joint Chiefs of Staff. (2018). *Joint publication 3-12, cyberspace operations*. Retrieved from https://fas.org/irp/doddir/dod/jp3_12.pdf

United States Department of Defense. (2015). *The DoD Cyber Strategy*. Retrieved from https://www.hsdl.org/?view&did=764848

United States Department of Defense, Defense Science Board. (2017). *Task force on cyber deterrence*. Retrieved from https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf

United States Department of Justice. (2014, May 19). U.S. charges five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage [Press release]. Retrieved from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

United States Department of Justice. (2016, March 24). Seven Iranians working for Islamic Revolutionary Guard Corps-affiliated entities charged for conducting coordinated campaign of cyberattacks against U.S. financial sector [Press release]. Retrieved from https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

United States Department of Justice. (2017, November 27). U.S. charges three Chinese hackers who work at internet security firm for hacking three corporations for commercial advantage [Press release]. Retrieved from https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

White House, The. (2003). *The national strategy to secure cyberspace*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

White House, The. (2011). *International strategy for cyberspace*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

White House, The. (2015). *The national security strategy*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

White House, The. (2017). *The national security strategy*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

White House, Office of the Press Secretary. (2013, June 17). *Fact sheet: U.S.-Russian cooperation on information and communications technology security* [Press release]. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol

Zetter, K. (2012, August 30). Qatari gas company hit with virus in wave of attacks on energy companies. *Wired*. Retrieved from https://www.wired.com/2012/08/hack-attack-strikes-rasgas/

Zetter, K. (2015, February 10). The NSA acknowledges what we all feared: Iran learns from US cyberattacks. *Wired*. Retrieved from https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired*. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California