International Master's Program in International Studies

National Chengchi University

國立政治大學國際研究英語碩士學位學程

# Warfare and Deterrence in the Cyber Realm: The Cases of the United States and Russia

# 網路戰爭與嚇阻：以美國與俄羅斯為例

Nicholas Sidman

Advisor: Yung-Fang Lin

June, 2018

DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

**Abstract**

This thesis examines the cyber operations of the United States and Russia. By examining these two separate states, and the individual cases related to their cyber development, I illustrate how notions of deterrence are developing in the cyber realm. A major problem currently facing states with regards to deterrence in cyber space, is attribution. Knowing who engages in what cyber operations is attribution. However, through analysis of United States and Russian cyber operations through the lens of Joseph Nye's approach to cyber operations and deterrence I illustrate that in the future the well known offensive advantage may lessen. Specifically, those actors besides well-organized and sufficiently funded nation-states may find cyber operations too costly and too risky to be of value. This is as a result of not just improved attribution technology, but also due to improvements in nation-state's cyber defensive postures and generally improved cyber hygiene. Further, attempts at bilateral and multilateral agreements with regards to cyber may further reduce operations; or at least, reduce operations outside of the purview of the intelligence services of various official actors. Ultimately, it is found that, in similar fashion to air power in the early 20th century and nuclear weapons in the middle of the 20th century, states will likely develop both tangible and intangible approaches to dealing with the threat of cyber operations. However, where status-quo powers like the United States embrace the adoption of legally binding multilateral treaties and agreements regarding cyber, other states such as Russia would rather not potentially lose an important part of what makes Hybrid Warfare operations viable. The debates on and development of cyber may involve two clear camps in the future, those supporting the status-quo and so-called revisionist powers.

**DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06**

# 摘要

本研究檢視了美國和俄羅斯的網路運作。透過檢視這兩個不同的國家以及與他們網路發展相關的個案，研究者舉例說明威嚇的概念是如何在網路領域中發展起來的。目前各國在網路空間的威嚇上面臨的主要問題是歸因問題，知道有哪些人參與網路運作即屬歸因問題。然而，透過約瑟夫·奈爾（Joseph Nye）對網路運作和威嚇的方法，對美國和俄羅斯的網路行動進行分析，我以實例說明未來眾所周知的攻擊性優勢可能會減少。具體而言，除了組織完善且資金充足的國家之外，其他參與者可能會發現網路運作成本太高、風險太大。這不僅是因為改進了歸因技術，而且還因為各國在網路防禦方面有所改善，並普遍改善了網路衛生。此外，有關網路的雙邊與多邊協議的嘗試可能會進一步減少網路運作攻擊，或至少，減少各種官方情報單位範圍以外的行動。最終，人們會發現與 20 世紀初的空軍戰力和 20 世紀中期的核武器類似，各國可能會開發有形和無形的方法來應對網路作戰的威脅。但是，在現今的強權國家如美國，接受有關網路之具有法律約束力的多邊條約和協議的情況下，俄羅斯等其他國家也不願意失去在使混合作戰行動中可行的重要角色。在未來，關於網路的爭論與發展可能涉及兩個明確的陣營，即指那些支持現狀和所謂修正主義的陣營。

DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

# Table of Contents





DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

## Chapter 1 Introduction

### 1.1 Research Motivation

The 20th century saw the beginning of airpower as an important and decisive aspect of all military campaigns. Military usage of aircraft began in the first World War, with reconnaissance in particular playing a key role. By the second World War, other technologies had arrived that further enhanced the military capabilities of aircraft. In particular, long-range strategic bombing was seen as a paradigm shift in multiple theaters. Air superiority became the key factor in winning campaigns; and even at sea, aircraft carriers supplanted the once fearsome battleships in terms of importance. However, with the rising capabilities of offensive airpower, there was also a corresponding development of defensive countermeasures. Loss rates on bombing sorties in the Second World War became extremely high as a result of improved anti-aircraft weaponry and improvements in air-to-air fighters tasked with aerial interdiction and defense missions. Further, advances in rocketry over the years have led to increasing balancing between offensive and defensive capabilities; for example, Russia's natively produced S-400 Triumf anti-aircraft weapons system is infamous and feared for its quality and its predecessor, the S-300, is still used around the world. In addition, advances in radar and early-warning systems have further deteriorated the offensive advantage of aircraft that was once theorized to be insurmountable. Now, a proper military doctrine requires a combined arms approach that protects valuable aerial assets through targeting these defensive measures.

Information and how it is gathered and used in military campaigns has also changed over



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

the course of the 20th century. This has accelerated greatly with advancements in networking and information technology, and to this day paradigms and doctrines are being written to account for the breakneck speed of development. Many may look at the first Gulf War as representing the peak of American power and hegemony; however, in addition to this it was one of the first truly modern conflicts of the computer age. Advanced technology was used to target Iraqi anti-aircraft assets and jamming tools were used to ensure a clear advantage for the Coalition Forces through complete air superiority. Diverse actors have looked to this conflict, and later actions by the North Atlantic Treaty Organization (NATO) in Kosovo, and devised new strategies and countermeasures to account for the overwhelming force that the United States and its allies can bring to bear on any adversary. The result has been something of a cyber arms race, with nation states valuing offensive capabilities and sophisticated hacking tools as an option for checking American hard power. One of the key actors in this space has been the Russian Federation. Beginning in 2007 with the cyberattacks on Estonia, followed by the 2008 Russo-Georgian War, and culminating in the conflict in Ukraine, Russia's use of Cyberwarfare has developed and sharpened into a trademark of their Hybrid Warfare approach. This has come about as a result of the United States' own cyber development and prowess, and was devised to counter a materially more powerful adversary. Now, the United States and its policy makers must devise a counter to these counters. This may come through a variety of deterrence avenues, likely focusing on improving attribution and network security, more and more embracing non-cyber responses to cyber affronts, and developing international norms that take into account Cyberwarfare and its pace of development.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

This paper will seek to better understand the formation of cyber policy and how it may develop in the future, in particular how deterrence theory will engage bleeding edge cyber operations.

### 1.2 Purpose of Research and Research Questions and Main Argument

The purpose of this research will be to better understand how cyber developed and how it is currently developing, and in particular, how nation states will develop doctrines and strategies to deter offensive hacking. In particular, I will study Russian and United States cyber policy, and how they have affected each other. How will the United States cyber policy and technology acquisitions change to meet Russian, and other nation-state and non nation-state, challenges.

In this paper, Cyberwarfare will be the key topic of discussion. Russian Information Warfare will be considered part and parcel of Cyberwarfare. Cyberwarfare in this paper will be, in a general sense, defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[1] These may include overt kinetic operations, such as attacks on infrastructure or weapons facilities like that of Stuxnet, or propaganda operations, like those of Russian origin in Ukraine and Georgia, or espionage operations, commonly carried out by Chinese operatives. Using this definition, the primary question will be how states, in particular the United States, may develop strategy and policy to deter future unfriendly operations.

Currently offensive hacking tools are numerous and powerful. This leaves those tasked

[1]Clarke, Richard A. and Robert K. Knake. Cyber War: The Next Threat to National Security and What To Do About It. New York, NY: Ecco, 2010: 6



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

with security in an uphill battle. Network security technology is still catching up with the capabilities of aggressive hackers. This is currently being done through a variety of means that essentially boil down to developing a more dynamic and active system of network security. Further, there is still not a clear doctrine on how to respond to incursions. However, like security technology and methods, this as well is developing. In combination, the hope is that future incursions will be deterred through making offensive operations too costly to consider for most actors, and/or providing a credible and real threat of retaliation; these responses could be either directly through counter-hacks or other means, such as economic sanctions.

This current problem of adequate deterrence is partly a result of the difficulty of attribution in cyberspace. It is difficult for investigators to determine who is hacking who and what their affiliations are; and without a clear target there is no way to counter-hack or respond in any productive fashion. However, progress is being made on the attribution front as more and more high-profile foreign operations are being uncovered and tracked by the US government and private security firms. Developing international legal norms may also be used by states to protect themselves in cyber-space. Currently, the international community is still developing the regulations and norms for cyberwarfare that conventional warfare has enjoyed for centuries. The United States as well may be able to take the lead here, and craft the regulations to their liking to improve deterrent capabilities. Cyberspace is still in a Wild West stage, however, even compared to just several years ago, network security technology and knowledge has improved and possible defensive policy measures have been used in the face of cyberattacks. For example, the United States placing further economic sanctions on the Russian Federation following the hacking



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

operations during the 2016 United States election is an example of using one kind of policy, separate from cyberspace, to punish transgressions in that realm. Presently, the Russian Federation and its cyber tactics have developed a fearsome reputation out of its ability to counter the foundational strategies of larger geopolitical opponents like the United States and, especially, NATO. However, over time, the United States will continue to advance technologically and strategically in the avenue of cyber and will devise counters to these Russian tactics. These include improving attribution capabilities and devising new international legal norms; that will shift the paradigm of cyber from pre-emptive and offensive focused to one that pays more attention to network security and countermeasures.

While offensive airpower was once dominant and paradigm shifting, counters were developed and balancing occurred; the same will happen in the realm of cyber, and the United States, thanks inadvertently to the development of Russia's own brand of hybrid warfare, will be the entity to lead this shift so as to maintain a position of cyber superiority in the future. Cyber will not develop in an offensive kinetic fashion due to the inherent difficulty and extreme costs associated with this approach. Instead, cyberdeterrence will become integrated with other government policies, such as economic sanctions, and propaganda and espionage operations will be the primary preoccupation of network security specialists. Defensive postures will become more and more stable and serve as an increasingly powerful deterrent as attribution technology improves.

### 1.3 Literature Review



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Moore's Law states that computing power will increase exponentially as the number of transistors that can fit onto a silicon chip doubles every year or two. Since this observation was made in 1965 the pace has not broken, and more and more of the armed forces and intelligence services of nation states around the world seek to take advantage of technology improvements to gain an advantage over their rivals. Russia and the United States are of particular interest due to their different approaches in using cyber to pursue a grand strategy.

Following the Cyberattacks on Estonia in 2007, the use of Cyberattacks in the Russo-Georgian War, and the use of Cyberattacks in the Ukraine and Crimea, many experts have weighed in on how significant cyber is for Russian campaigns and how it is now an important part of Russia's Grand Strategy in its near abroad. Many authors note that while much buzz is made in the western media regarding Russia and its use of cyber, in reality the Russian perspective does not differentiate between "Cyberwarfare" and "Information Warfare"[2]. Instead, similar to the Soviet era, cyber is included within the domain of "Information Warfare" and used in a similar fashion. While targeted attacks to infrastructure may be made, generally Russian forces seek to capture useful information on opponents and create a "Fog of War" through cyber deception. However, authors have also noted that as Russian expertise has increased, targeted destructive attacks could be undertaken[3].

[2]Giles, Keir. "'Information Troops' – a Russian Cyber Command?" Presented at the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011. http://conflictstudies.org.uk/files/Russian_Cyber_Command.pdf

[3]Weedon, Jen. "Beyond 'Cyber War'" Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, 67-78. Tallinn: NATO CCD COE Publication, 2015.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

This "Information Warfare" can be seen both locally in Ukraine/Crimea and abroad, with election hacks and funding for both far-right and far-left parties throughout Europe, along with a government funded detachment of internet "trolls." Further, at home, Russian texts frequently regard cyber as an existential threat where Russia is actually supremely vulnerable to outside forces. If Russian policy-makers do indeed view Russia as vulnerable in the realm of cyber, state actions often do not align with these expectations. It has been suggested that Russia's current aggressive policies, both on the ground and in cyberspace, reflect one of Stephen van Evera's explanations for why states go to war, defensive expansionism[4].

This explanation for Russian geopolitical actions is further strengthened when viewing Europe as a contest between Russia and NATO/The United States. Russia has tailored its Cyber strategy to bypass the deterring tripwires of NATO. For example, by creating a Fog of War in Crimea and Eastern Ukraine, maintaining plausible or implausible deniability, and by controlling flows of information into and out of these areas, Russia was able to delay any western responses and establish boots and facts on the ground. With an established presence in Eastern Ukraine and Crimea, the cost of western escalation has risen greatly[5]. Therefore, it can be argued that Russia's cyber strategy, and Grand Strategy, is tailored specifically towards defeating NATO and western influences and protecting its near abroad.

[4]Medvedev, Sergei A. "Offense-Defense Theory Analysis of Russian Cyber Capability." Master's Thesis, Naval Postgraduate School, 2015. http://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf?sequence=1

[5]Wirtz, James J. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, 29-38. Tallinn: NATO CCD COE Publication, 2015.

https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

The United States has frequently been described as a nation under severe cyber attack from media outlets, but in reality the United States maintains a clear advantage in the realm of cyber. As many leaks and reports have shown, the United States has a wide variety of sophisticated offensive hacking tools that can both obtain information and engage in targeted attacks with little risk of reprisal. For the cyber hegemon, the greatest preoccupation is network security and maintaining its preeminent status. While Russia and China both acknowledge their own weaknesses and seek to tailor their strategies around this deficiency through offensive cyber development, the United States faces the opposite problem. One major issue with devising defensive strategies of deterrence is the problem of attribution inherent in cyber activities. If Russian hackers can operate out of Nigeria using techniques that are more associated with Chinese government operatives to target critical United States systems, how can network security operatives quickly find the culprits and recommend adequate responses. Legal norms have been suggested as a means of deterring future cyber attacks[6], however this all requires adequate attribution. A more comprehensive deterrence structure would involve technical approaches such as dispersing networks, IP hopping, use of the Cloud, data fractioning, and others, while able to detect and immediately respond to attackers in asymetric ways. This would involve keeping active defense measures in place 24 hours a day. This multifaceted approach would deter through difficulty in the act of hacking, and the immediate response that could be expected from a network's defenders[7].

[6]Lotrionte, Catherine. "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence." *Georgetown Journal of International Affairs* Special Cyber Issue, 3rd ed. (January 2014): 71-84. http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13007_Lotrionte- CYBER-III.pdf

[7]Fahrenkrug, David T. "Countering the Offensive Advantage in Cyberspace: An Integrated



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

United States cyber power was most evident to the world with the Stuxnet attacks on Iranian nuclear facilities. However, in retrospect, there has been much debate on whether the attacks themselves were valuable and whether these kinetic attacks will be an important aspect of cyber activities in the future. Empirical studies on kinetic attacks flip the common script of weaker powers directly attacking the infrastructure of larger powers. Instead, the high costs and marginal benefits of these attacks reveal that while kinetic attacks are an option for wealthy powers, they often will not have the catastrophic results that many envision[8]. Rather, these targeted attacks, when taking Stuxnet as the prime example, may marginally slow or hamper a target. The development and operational costs for these targeted attacks will generally outweigh benefits except for top powers like the United States[9]. However, if the costs of offensive hacks were to decline and defensive measures were not improved, even the United States and its infrastructure would be at risk of sabotage from rival powers[10]; although it is noted that this power is still out of reach for most operators[11]. A caveat with kinetic attacks to also be considered, is that with clandestine cyber attacks the physical results may not be of the utmost importance. Instead, the messages and changes in perceptions may be the end goal; messages and perceptions that may alter later diplomatic proceedings. This empirical analysis calls into

Defensive Strategy." Presented at the 4th International Conference on Cyber Conflict, Tallinn, Estonia, 2013. https://ccdcoe.org/cycon/2012/proceedings/fahrenkrug.pdf

8 Slayton, Rebecca. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* Vol. 41 Issue 3 (Winter 2016/17): 72-109.

9 Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* Vol. 22, Issue 3 (2013): 365-404.

10 Applegate, Scott D. "The Dawn of Kinetic Cyber." Presented at the 5th International Conference on Cyber Conflict, Tallin, Estonia, 2013. https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf
Baylon, Caroline, Roger Brunt, and David Livingstone. "Cyber Security at Civil Nuclear Facilities: Understanding the Risk." Chatham House. 2015.

11 Clayton, Blake and Adam Segal. "Addressing Cyber Threats to Oil and Gas Suppliers." Council on Foreign Relations. 2013.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

question future doctrine and strengthens the argument that the future of cyber will not be kinetic and offensive, but rather will focus on espionage and information conflicts while large powers strive to maintain a secure network through an advanced defensive posture.

Cyber and Information War itself has been a subject of debate by academics and industry leaders. Of particular mention has been the discussions of whether offense will overwhelm defensive measures or vice-versa in the future. Generally speaking, authors agree that it is currently all but impossible to stop cyber incursions from motivated attackers[12]. While commonality is found with regards to the current power of offensive operators, the most interesting analysis is regarding how embattled states may craft policy to deter hackers. Approaching hacks from a cost/benefit perspective, as suggested by Nye[13], as opposed to purely from an absolute power dynamic would be an appropriate approach in researching what may lead to a more stable world. Many authors will analyze singular factors that may lead to deterrence, such as legislation, norms, active defense, and others; however, Nye and Slayton have offered cumulative studies that illustrate the subtlety of cyber operations. It is likely that in the coming years as this research becomes more advanced and political scientists more aware of technological advances, the literature will become more focused on the gray areas that make cyber and deterrence so difficult to reconcile when compared to nuclear and conventional weapons. In particular, a focus on the need for a combination of policies to provide adequate

[12] Junio, Timothy J. "How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate." *Journal of Strategic Studies,* (2013).
Libicki, Martin C., Lillian Ablon, Timm Webb. "The Defender's Dilemma: Charting a Course Toward Cybersecurity." RAND Corporation. 2016.

[13] Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* Vol. 41 Issue 3 (Winter 2016/17): 44-71.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

deterrence as opposed to simply more offensive capabilities, active defenses, or international norms individually. Lastly, as mentioned by Nye, attempts at complete deterrence will likely change and researchers may engage with models from other disciplines, such as public health models, in dealing with illicit cyber activity; focusing on gradual harm reduction instead of complete deterrence.

Some authors, discussing policy, have suggested a more "active defense" that acts as a primary deterrent[14]. This policy has also been criticized because of attribution issues, risks arising from too hawkish a stance, amongst others[15]. Other authors have offered research on using norms building and legislation to respond to cyber attacks and/or espionage and deter future attacks[16]. Although, the likely best simple and quick policy options would be further research on and hardening of local networks and, more importantly, proper training for staff in handling sensitive materials. Many hacks are as a result of human error, and are as simple as using an infected USB stick or clicking on a spam e-mail. This avenue would likely offer the most immediate results, given the rudimentary means that many hackers are using to infect even secure networks.

Cyberwarfare will continue to gain importance as each year passes, and every nation state

[14] Rivera, Jason, and Forrest Hare. "The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures." Presented at the 6th International Conference on Cyber Conflict, Tallinn, Estonia

[15] Geist, Edward. "Deterrence Stability in the Cyber Age." *Strategic Studies Quarterly,* (Winter 2015): 44-62.
Hathaway, Oona A. "The Drawbacks and Dangers of Active Defense." Presented at the 6th International Conference on Cyber Conflict, Tallinn, Estonia, 2014.

[16] Demchak, Chris C. and Peter J. Dombrowski. "Rise of a Cybered Westphalian Age". *Strategic Studies Quarterly*, (Spring 2011): 31-62.
Buchan, Russell. "The International Legal Regulation of State-Sponsored Cyber Espionage." In *International Cyber Norms: Legal, policy & Industry Perspectives* edited by Anna-Maria Osula and Henry Rõigas, 65-86. Tallinn: NATO CCD COE Publication, 2016.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

will devise their own cyber-strategy tailored towards their own goals. The Russian and United States cases show that different material and historical circumstances will affect policy in this regard, in addition to perceptions of power disparities. Of most interest, however, is how advancements in the United States may tip the balance from an offensive focused cyber paradigm to one that more explicitly favors defense and may one day lead to the development of a legal norms based and holistic approach to cyberincursions that may act as an adequate deterrent.





DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

## Chapter 2 Theoretical Framework

The following chapter will first introduce deterrence theory and the reasoning for its importance to the topic will be explained. Following a general discussion of deterrence theory, specific aspects devised by Joseph Nye will be contextualized into a cyber paradigm. The author will then explain how these aspects will be used in this analysis. Next, the author will then note and describe the specific qualitative methods used in this paper and will note and describe the variety of sources used and why. Next will be a short section on technical aspects of the subject.

### 2.1 Deterrence Theory

The author will be approaching the question of the paper, how will United States cyber policy change in the future; and will the policy changes be more offensively or defensively oriented, with the aid of Deterrence Theory. Deterrence Theory has been discussed and debated for hundreds of years, however it gained great significance during the Cold War. In particular, the idea of a nuclear powered state fending off the aggressions of a non-nuclear and otherwise significantly more powerful enemy state. Thomas Schelling's work, *Arms and Influence*, contributed greatly to Deterrence theory; arguing that in modern day international relations, military strategy now included concepts of coercion, intimidation, and deterrence.[17] Further, many theorists would approach Deterrence using Rational Choice theory and especially Game Theory modeling. It was from these approaches that many scholars would engage in studies of arms control and nuclear stockpiles; which would lead to further studies, quantitative and qualitative, on first-strike, second-strike capabilities and so on. The end of the 20th century and the Cold War provided a fertile ground for this research, as the International Community was

[17] Schelling, Thomas C. *Arms and Influence*. Yale University Press, 1966. http://www.jstor.org/stable/j.ctt5vm52s.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

split between East and West. This allowed for academics to assume rationality on the part of the United States and the Soviet Union, respectively; as both powers were seeking similar goals.

However, Deterrence theory has faced frequent criticisms throughout the 20th and 21st centuries. Some of the most common include the situation wherein an irrational opponent cannot be deterred outright, the situation where one nation attempts to gain a surprise first-strike advantage over its opponent, diplomatic bungling may lead to increased perceptions and misconceptions of threat which may lead to an arms race; an inefficient result, and that heightened perceived threats would allow governments to impose measures on its citizenry such as limitations on civil liberties, increased deficits and taxes, and the creation of a military-industrial complex. Much modern criticism focused on the irrationality of many threats. For example, as suicide bombings and ideological conflicts have become the new normal, these opponents are unlikely to be deterred by traditional means. As a result, many states have reduced their nuclear stockpiles and pursued a policy of minimal deterrence, where only enough of a stockpile is maintained to prevent attacks.[18] This, in contrast to mutually assured destruction, where any attack would lead to a retaliation using full force. Further, as conflicts have become more and more regional, nuclear weapons have less deterrence value compared to in a conflict like the Cold War. Some analysts now see the nuclear age as passing, and cyber taking its place.[19] In particular, the destructive power of various hacks and the damage that could be wrought on a domestic audience if classified documents were released that altered political

[18] Kristensen, Hans M., Norris, Robert S., and Ivan Oelrich. "From Counterforce to Minimal Deterrence: A New Nuclear Policy on the Path Toward Eliminating Nuclear Weapons." Federation of American Scientists and The Natural Resources Defense Council. Occasional Paper No. 7. April 2009. https://fas.org/pubs/_docs/occasionalpaper7.pdf

[19] Virilio, Paulo. "The Kosovo War Took Place in Orbital Space." Interview by John Armitage. CTheory. October 18, 2000. Accessed March 26, 2018. http://www.ctheory.net/articles.aspx?id=132.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

processes. It is then timely to note that the 2016 United States election was mired in this sort of controversy. From this, it seems important to approach deterrence in a different and more evolved manner. In particular, focusing not on the assured destructive capabilities of nuclear weapons but on the longer term and more subtle damage that cyber operations can inflict.

**2.2 Deterrence Theory and Cyber Context**

The author will approach deterrence in the cyber realm in a similar fashion to the earlier mentioned Joseph Nye article; in particular disregarding fanciful ideas of total prevention and focusing on a reduction of incursions and dissuasion. Nye lists "four major mechanisms to reduce and prevent adverse actions in cyberspace: threat of punishment, denial by defense, entanglement, and normative taboos," and also notes the latter two are not strictly considered deterrence; although views them as important and useful from a policy perspective.

Punishments are the direct retaliatory use of force against aggressors, or more accurately, the threat of retaliation that will deter aggression. Punishment in the cyber realm is also the most difficult as a result of attribution issues and, in the United States, a reticence to reveal offensive capabilities to the general public. However, while deterrence through punishment is difficult and frequently criticized in cyberspace, it is still a valid option and may grow in importance if attribution capabilities also improve.

Denial by defense as deterrence is increasingly gaining in importance as cyber operations are approached in less absolute terms. Hardening of important systems and developing resilience and recovery capabilities changes the value judgements of attackers. Where previously cyber operations may have been effective and cost efficient, if cyber defenses improve then future



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

attackers may be dissuaded due to the low chances of success. Further, if systems are hardened and easily recoverable, there is even less value in aggressive infiltration operations and the risks to the attackers of retaliation further alter the calculations. Nye discusses this aspect of deterrence in cyber by bringing up disparate fields, such as public health models, where proper "cyber hygiene" may aid in preventing unsophisticated hackers from affecting important systems. While more sophisticated attacks may get through, if the majority can be prevented through improved defensive measures that is progress.

In addition to mechanisms of classical deterrence, Nye also looks to Glenn Snyder's definition and concept of "Broad Deterrence" that includes ideas of entanglement and norms. Entanglement, as used by Nye, "refers to the existence of various interdependencies that make a successful attack simultaneously impose serious costs on the attacker as well as the victim." An example in the world of cyber would include a hostile power not engaging in aggressive cyber operations due to the value of the internet and a global open cyberspace to their economy. There are examples of this phenomenon occurring in other areas as well, particularly between great states that are competing economically and militarily. This additional factor is interesting to examine when analyzing the future of cyber, the internet, and economies. As the internet and technology contributes more and more to economies around the world, entanglement may reduce state sponsored operations in favor of fostering an open and profitable environment.

Norms and taboos are in the earliest stages of development with regards to cyber. Past examples in history would be with regards to nuclear weapons. While tactical nuclear weapons and miniaturized versions were considered for conventional usage, over time the concept fell out



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

of favor and in the present nuclear weapons are seen as a last resort option that should never be used except for in the rarest of instances. If a state were to use nuclear weapons, unless circumstances were dire, they would assuredly receive international condemnation. Cyber may also develop these elements if nation states take the lead to proactively put limits on how cyber will be used in the future. Similarities could be seen to biological and chemical weapons bans and agreements, where while some actors did maintain and use them, they were considered to be largely taboo in the international community. The United States and Chinese governments have offered international legislation in this direction, although currently there is still little beyond the beginnings of norms development.

From this theoretical approach, the author will analyze the respective subjects and their unique cases. In the case of the United States, there are also points that may be examined through this framework. Threat of punishment has developed a growing group of supporters in the United States, and it all ties into how attribution technology will develop to aid in this strategy. Denial by defense has also been improving, as a new cyber posture is developing in the United States armed forces and new technology is being rolled out for this specific purpose. Entanglement may be seen in how the United States approaches its interactions with Russia, and other major states, to deter future hacks. For example, direct negotiations with foreign officials on this subject, and in particular China.[20] Lastly, the United States has been involved in developing norms and taboos with foreign powers to reduce cyber incursions, especially with China because of the strong economic ties found between the two nations.

[20] Harold, Scott W. "The U.S.-China Cyber Agreement: A Good First Step." *The Rand Blog* (blog), August 1, 2016. Accessed March 26, 2018. https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

In the case of Russia, one can examine all four points. Regarding threats of punishment, it is most interesting to examine how Russia has used cyber to undermine traditional notions of deterrence by its geopolitical rivals.[21] Further, it has maintained cyber capabilities that likely prevent operations from rivals such as Ukraine and Georgia. Russia has also managed to break through many states defenses, leaving many scrambling to develop better denial capabilities. Entanglement is also likely at play, preventing Russian operatives from engaging in direct kinetic cyber operations in already compromised systems, for example in Ukraine.[22] Norms and taboos may also be involved, as Russian operatives are not known for kinetic operations. This may be because of an inherent fear of reprisals in that regard. The author will more fully elucidate all of these points in each state's respective chapter.

**2.3 Research Methods**

The author will approach this research qualitatively, focusing on cases involving Russian and United States cyber operations. These subjects are, along with North Korea and China, some of the most powerful and visible cyber players in the world. As such, there is a wealth of history and research on specific events and these states respective cyber postures and infrastructures. In particular, the author will be examining Russian cyber operations during the Estonian Cyber Attacks, the Russo-Georgian War, and the conflicts in Ukraine and Crimea. Russian cyber operations are important to analyze because they are some of the only examples that have

[21] Wirtz, James J. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, 29-38. Tallinn: NATO CCD COE Publication, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf

[22] Roigas, Henry "The Ukraine Crisis as a Test for Proposed Cyber Norms." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, 135-144. Tallinn: NATO CCD COE Publication, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Roigas_15.pdf



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

occurred in hot conflicts. Further, the methods used by Russian operatives is arguably designed to degrade and weaken previous notions of deterrence in Eastern Europe and to degrade and weaken any opponents to Russian preeminence in their near abroad. This aspect of Russian cyber operations directly allows for further discussions of deterrence and how it will operate and be used in a new and developing cyber paradigm.

The author will also be examining United States operations and, in particular, how United States cyber policy has shifted to account for a changing Russian threat. An interesting aspect of the relations between the United States and Russia has been a long studied history of conflict. Or to simplify, the later stages of the 20th century were shaped by the Cold War and the competition between the West and the East. In particular, modern deterrence studies emerged from this competition; and it was further bolstered by the nuclear bomb and its coinciding fears. Now, new technologies are emerging that raise further questions regarding the viability of deterrence and what the relationship between the United States and Russia will look like in the future. In addition, the United States approach to cyber is vastly different from its Russian counterpart. Russian operations are often more based on a concept of Information Warfare and propaganda.[23] In contrast United States operations owe more to Clausewitzian concepts of decisive battles and have involved direct kinetic attacks; one of the top examples being the Stuxnet computer worm that targeted Iranian nuclear facilities. This computer worm was precisely targeted and destructive in its intent. This differs greatly from Russian Information and Propaganda operations.

[23] Giles, Keir, "Russia's Public Stance on Cyberspace Issues," presented at the 4th International Conference on Cyber Conflict, Tallinn: Cooperative Cyber Defense Centre of Excellence (2012): 63-74, https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

However, as technology improves conceptions of Cyber are changing. Past operations have, as stated, conformed to prior ideologies of warfare that were also culturally biased. For example, Russian Cyber operations have largely been based on controlling and manipulating information. This Information Warfare has been a key strategy since the Soviet era, and continues to the present; even going as far as potentially affecting United States electoral proceedings. In contrast, the United States has been more kinetic and often used to support combat operations. Further, these operations were placed within conventional warfare and diplomatic paradigms. The new technology was an additional tool, not yet causing paradigm shifts of its own. However, as technology continues to improve, cyber may break away further and begin to change previous paradigms; similar to airpower in the early 20th century alluded to earlier in this paper. The United States and Russia are two of the leading actors in cyberspace, and as a result are the best subjects of study to determine whether Cyber is changing and how ideas of deterrence may or may not be changed.

**2.4 Sources**

This paper will make use of a variety of sources, primary and secondary. It must be noted, however, that due to the constantly changing and also clandestine nature of current cyber operations, official government documents are scant and in many cases third-party research groups and individual scholars are providing the bulk of useful information. For example, the United States has an official Cyber Command and issues reports and public information regarding doctrine and, rarely, capabilities[24]. In contrast, the Russian state apparatus is much

[24] "U.S. Cyber Command (USCYBERCOM)." United States Strategic Command. September 30, 2016. Accessed March 27, 2018. http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

more tight-lipped and it falls to the aforementioned third-party research groups to provide adequate information for analysis[25]. When analyzing Russian operations it is possible to look to past doctrines and documents for guidance. For example, because Cyber is still viewed within older paradigms, it is possible to use notes on Information Warfare and Propaganda to assist in understanding how Cyber is currently being used and may be used in the future by Russian operatives.[26] The United States, while being much more public in its Cyber operations, is also similar. There is a large history of intelligence operations and military doctrines that provide a framework for analyzing current Cyber operations. However, as noted earlier, as paradigms change this prior history may no longer be relevant in analyzing cyber and its affects on policy.

Outside of official documents, the secondary sources will be comprised of a variety of research groups, think tanks, and commercial groups. The author will frequently make use of analysis from The Tallinn Manual[27], an ongoing study on how international law applies to cyber conflicts and cyber wars. The research group is composed of a variety of subject matter experts and led by Professor Michael N. Schmitt, professor at the United States Naval War College and the University of Exeter; other contributors include various academics from the United States and Europe, United Kingdom Royal Air Force officers, Canadian military officials, and United States military officials. Prior to its initial publication, the Tallinn Manual was peer-reviewed by fellow international legal scholars. The Tallinn Manual was written at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence, although the study and views

[25] Giles, Keir. "'Information Troops' – a Russian Cyber Command?"

[26] Heickerö, Roland. (2018). FOI Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.

[27] Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. doi:10.1017/CBO9781139169288.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

contained within are considered independent of official NATO policy. The Tallinn Manual is an important source of information because it is one of the first attempts at studying the legal dimensions of Cyber Conflict and how to apply international law to these matters. In 2017 a Tallinn Manual 2.0 was released, focusing on Cyber legality questions below the level of destructive conflict.[28]

The author will make use of peer-reviewed articles focusing on more theoretical and less technical aspects of Cyber and its changing paradigms. Some of the journals included will be Strategic Studies Quarterly, the Journal of Strategic Studies, Security Studies, International Security, and others. These articles will offer both a broader analysis of Cyber operations and how it relates to theory and more narrow analysis and research of specific cases and events. In particular, when examining Deterrence and how it will operate in a Cyber paradigm, these articles will be extremely useful. However, because of the technical nature of Cyber operations and the generally less technically savvy nature of Political Science and International Relations, there cannot be a complete understanding of the subject without also engaging with technical experts and computer science experts. That is the primary deficiency of purely engaging with Social Science on this subject. The author will make use of more technical journals to bridge this gap. Some of these will include Network Security, Computers & Security, IEEE Security & Privacy, amongst others. The goal will be to bridge the gap between hard and soft sciences as well as possible.

As alluded to, the author will also make use of various commercial technical reports on

[28] Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. doi:10.1017/9781316822524.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

hacks and various other cyber operations. One of the most cited companies will be FireEye, Inc. FireEye is an American cybersecurity company that provides security products and services against more advanced threats. The company has also been hired to research high-profile hacks of companies such as Sony Pictures, Target, and JP Morgan Chase, amongst others. FireEye is also known for publishing Advanced Persistent Threat reports. These APT reports analyze hacking operations waged by nation states, and have exposed North Korean, Iranian, Russian, and Chinese operations.[29] The APT 28 report, in particular, sheds much light on current Russian cyber operations and their technical attributes.[30] Also of note, the FireEye researchers often collaborate with universities and governments in their assignments.

**2.5 Technical Discussion and Problems**

The technical nature of this subject results in some unique features that require explanation. When analyzing Cyber operations, it is important to understand the various means that are used to complete objectives and how sophisticated operators may differ from amateurs. For amateurs, the goal is often to cause havoc for individual amusement, support a greater cause, or possibly seek monetary gains through illicit means. These operators will often make use of more rudimentary tools, such as various types of malware, or rudimentary methods, such as phishing, to achieve their goals. Phishing is an attempt to obtain sensitive information online by disguising oneself as a trustworthy entity. The more advanced form is known as Spear-Phishing, where entities attempt to obtain sensitive information from specific targets. It is common for hackers to

[29] "Advanced Persistent Threat Groups." FireEye. Accessed March 27, 2018. https://www.fireeye.com/current-threats/apt-groups.html.

[30] APT28—A Window Into Russia's Cyber Espionage Operations?. Special Report. FireEye, 2014. https://www2.fireeye.com/apt28.html.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

use false emails or websites to gather this information. In some cases, however, these amateur users may receive more advanced hacking tools from separate entities. For example, this has been an alleged practice of Russian government officers; dispersing more advanced tools to the public in order to achieve geopolitical objectives.[31] More advanced criminal groups generally operate with the goal of enriching themselves financially; although some nation states will allegedly do the same.[32] Often operations involve targeting the personal information of customers of large corporations. Once breached, this data may be sold on the black market. This has occurred frequently in the past decade to major companies such as Target, Yahoo, and Equifax. In addition, criminal groups may seek out exploits and design their own hacks; which they may then sell for a profit on the black market.

Nation states will differ from individuals and unaffiliated groups in terms of why and how they engage in cyber operations. For the why, nation states generally have some geopolitical goals that motivate their cyber operations. For example, Russian operatives may want to destabilize unfriendly neighbors or add another layer of plausible deniability to their operations. On the other hand, United States operatives may directly target specific items for destruction through kinetic means, as was the case in Iran. Generally speaking, the why is simply to pursue national interests. The how is where differences appear. These differences may result from disparities in technical abilities and even cultural aspects may affect how cyber operations are undertaken by separate nations.

[31] Bumgarner, John and Scott Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008" United States Cyber Consequences Unit, August, 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber- Campaign-Overview.pdf

[32] Cordesman, Anthony H. with the assistance of Charles Ayers. *Korean Special, Asymetric, and Paramilitary Forces*. Washington, DC: Center for Strategic and International Studies, 2016. 29. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160809_Korean_Special_Asymmetric_Paramilitary_Forces.pdf



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

The United States and its level of technical prowess is difficult to properly contextualize. One example of the high level of technical abilities can be found in the EternalBlue exploit developed by the National Security Agency.[33] This exploit, targeting all Microsoft Windows versions prior to 8, was initially used to gather intelligence from targets worldwide. While extremely successful in this mission over the course of roughly five years, it was later stolen and released into the wild. This resulted in the subsequent worldwide spread of the WannaCry virus, that was one of the most disruptive in history. The WannaCry virus was developed using aspects of the EternalBlue exploit taking advantage of vulnerable Microsoft users; although, the goal of this virus was largely financial gain rather than to gather information. Another example would be that of Stuxnet, the computer worm that targeted and disabled Iranian centrifuges in a rare kinetic-style attack. As these varied operations show, the United States is far and away the most dangerous and proficient cyber power in the world. Most cyber operations are undertaken by the NSA, and involve cutting edge exploits to gather sensitive intelligence. A common technique used by NSA researchers involves finding zero-day exploits. These are exploits that take advantage of computer-software vulnerabilities and are completely unknown to those that would be interested in fixing said exploits. This includes the software and computer companies themselves, as seen in the earlier example of EternalBlue, where the NSA exploited Microsoft Windows vulnerabilities without notifying Microsoft. United States intelligence gathering is further enhanced by programs such as PRISM and MUSCULAR and alliances such as Five

[33] Nakashima, Ellen, and Craig Timberg. "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did." *Washington Post*, May 16, 2017. Accessed March 24, 2018. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.4ec69cfa3812.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Eyes. PRISM is the much written about program wherein the NSA gathers data from various United States internet companies such as Yahoo and Google. However, it should be noted that with PRISM, there are legal processes involved in data collection. MUSCULAR is another data collection program wherein the NSA and British Government Communications Headquarters clandestinely broke into communication links that connect data centers for Yahoo and Google. MUSCULAR requires no warrants because of its clandestine nature and as a result has collected twice as many data points when compared to PRISM.[34] These are only some of the programs that have come to light, it would be unlikely for there not to be other intelligence gathering programs active. Five Eyes is an intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom, and the United States. It is one of the most comprehensive and successful intelligence gathering alliances in the world and Five Eyes nations jointly run intelligence gathering programs such as PRISM and MUSCULAR.

In addition to intelligence collection through zero-day exploits, the United States has also shown an ability to engage in kinetic style attacks when needed. The most famous example of this is found in the Stuxnet worm, previously mentioned. The Stuxnet worm was developed to target Iranian nuclear centrifuges, and ultimately infected hundreds of thousands of computers and caused 1,000 machines to be damaged. The design of the worm itself made use of zero-day exploits, however its introduction to Iranian computers was likely carried out through an infected USB disk. A computer worm is a self-replicating computer program that may spread to other

[34] Gellman, Barton, and Ashkan Soltani. "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." *Washington Post*, October 30, 2013. Accessed March 24, 2018. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.12576195b082.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

devices and when spread executes commands. In the case of Stuxnet, this was to manipulate centrifuge operating systems and cause direct damage.

Lastly, the United States likely has its own Advanced Persistent Threats targeting various nations. An Advanced Persistent Threat is a long-term stealth hack, wherein operators work on a normal schedule to discretely retrieve data from the target. The term itself may refer to traditional espionage or attacks, but generally is used to refer to long-term intelligence missions. Targets may range from governments to private businesses. Most current writing will refer to Russian and Chinese led Advanced Persistent Threats that have been discovered, although it would be hard to discount the strong possibility of United States operators engaging in this approach as well.

Russian approaches to cyber operations have so far differed from United States approaches. This is likely due to separate geopolitical objectives, as well as a historical context that does not separate cyber operations from conventional operations as clearly as its American counterparts. There are two primary types of operations that have become signatures of Russian intelligence in the past decades. The first has been waging Information War, which in combination with other operations becomes the trademark Hybrid Warfare. Russian operatives are known for manipulating ingoing and outgoing information from target areas along with conventional and irregular combat operations to pursue national interests without attribution and/or retribution. Examples of this approach are common in the past decades, culminating in Ukraine, where Russian forces were able to disguise and muddy available intelligence long enough to establish boots on the ground. The cyber aspect of this Hybrid Warfare owes much to



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

the Soviet legacy of Information Warfare and propaganda. Russian forces use cyber methods such as fake news and other types of subversion through the mass media to influence various populaces. A second important type of operation are the previously mentioned Advanced Persistent Threats. One of the most famous is known as Cozy Bear, or advanced persistent threat APT29. APT29 was implicated in the spear-phishing campaign against the Pentagon in 2015, the Democratic National Committee hacks in 2016, and in attempting to hack into various other government databases.[35] Russian APT's are, along with Chinese, considered some of the most proficient in the world.

In a cyber landscape that sees security threats growing in number each year, it is more important than ever to pursue adequate defensive measures. The easiest way to immediately see defensive gains is through simple cyber hygiene. This involves frequent internal educational programs and testing for government workers. Developing awareness of what Phishing is and why to avoid strange USB sticks or other possibly compromised materials would help the most in the short term. In the medium term, developing a strong defensive cyber posture would help greatly in reducing incursions. This would be as a result of multiple factors. Firstly, a more secure network will inherently ward off attack attempts because of the time required to penetrate secure systems. Time would be better off spent pursuing other objectives. Secondly, a more secure network would simply be harder to penetrate if attempts were made. Long-term, accurate attribution of attackers would tip the balance further towards the defender. If hostile operators were able to be identified and shamed, this would cut down on attempts because there would be

[35] HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group. Special Report. FireEye, 2015. https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

an inherent risk associated with hacking. Currently, there is a small element of risk, but attribution technology has not advanced enough to consistently attribute hacks to the hackers in a timely manner.

Attribution is one of the largest problems facing network security experts. There are currently several ways to attribute an attack. One involves analyzing the source data, such as the IP addresses of the attackers or even emails. However, this information can easily be falsified to provide a false trail. Another involves analyzing the actual programming of the malicious software. For example, maybe the software was written on a Cyrillic keyboard, linking the attacks to Russian operatives. However, again, this is information that could be planted to provide a false trail for forensic analysts. A third option involves analyzing the behavior of the attackers. For example, if the attacker is an Advanced Persistent Threat, if they operate during regular government business hours in China consistently, it is likely of Chinese origin. Another option involves analyzing what was attacked or what data was taken. Sensitive financial information likely leads to criminal enterprises, whereas sensitive personal information on specific government officials would likely lead to a nation-state actor. Lastly, analysts may consider larger geopolitical factors in attributing hacks. For example, if a regime is currently under harsh sanctions and needs untraceable liquid assets, it may target bitcoin repositories or attempt to find other means of obtaining financial assets. Attribution currently is largely a guessing game and highly speculative, as it is extremely difficult to completely and conclusively attribute attacks. Without conclusive evidence of wrongdoing, it is impossible to punish a transgressor, and without any forms of penalty for cyber wrongdoing attackers will continue to



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

operate with relative impunity. Further, when it is borderline impossible to conclusively attribute certain operations to certain nations, this impacts how security and threat reports may be analyzed by scholars.






DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

## Chapter 3 The United States

The United States currently finds itself as the preeminent cyber power. This status has come about thanks to decades of research and development. Beginning in the 1960s, computer scientists began to explore new ideas that would become the foundation of the modern internet. One of the most important iterations was the Advanced Research Projects Agency Network, also dubbed as ARPANET. This project was initially tasked with connecting academic and military networks around the United States and later the world. It quickly flourished and added more members throughout the 1970s and 1980s, largely consisting of universities and government hosts. Meanwhile, network designs were also being further developed and the Internet Protocol Suite we now use today appeared. The Internet Protocol Suite is the model and set of protocols that are used on the internet. Essentially, the Internet Protocol Suite, or TCP/IP, determines how data should be transmitted and received. In 1982, the Internet Protocol Suite was standardized, allowing for worldwide proliferation of interconnected networks.

At its core, the internet and modern networking owes much to the United States military and its support. Its development was thanks to Department of Defense funding, and while its later iterations were less focused in scope, initially the concept was developed with the Cold War in mind.[36] This American focus on technology and its military uses would be clear in the latter stages of the 20th century and into the 21st. The First Gulf War in many ways introduced the world to modern warfare. The United States military, after heavy reorganizations and rethinking following Vietnam, and its allies repelled Iraqi forces from Kuwait and dominated the tactical landscape with extremely low casualties. This was thanks to a number of reasons that have been

[36]"Paul Baran and the Origins of the Internet." Rand Corporation. https://www.rand.org/about/history/baran.list.html



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

discussed and debated at length; and one of the key reasons cited has been technological developments and how they have been integrated into United States military operations.[37] The United States and its coalition allies in Iraq were able to establish complete air superiority, monitor Iraqi forces, communicate between themselves, and spy on Iraqi communications with impunity. Essentially, coalition forces had developed technology that eliminated one of the most dangerous aspects of warfare, the Fog of War. The incredible success of the campaign would put the world on notice regarding how wars would be fought in the future.

In 1999, NATO countries began a bombing campaign during the Kosovo War. This campaign would result in a NATO tactical victory, however, the political ramifications would extend to the present. Specifically, the NATO bombing campaign was not cleared by the United Nations Security Council, with Russia and China vetoing operations.[38] As a result, this was the first instance of NATO using military force without United Nations Security Council approval. More importantly, western actions in this politically sensitive region would make clear to Russian policy-makers that they could not rely on goodwill and international organizations to prevent possible incursions into their own near abroad; in addition, the technological superiority of western forces would impose a greater threat to Russian interests as time went on, if a strategy was not devised to counter these actors.

Russia would go through stages of warmer and colder relations with the United States in

[37] Biddle, Stephen. "The Gulf War Debate Redux: Why Skill and Technology Are the Right Answer." *International Security 22,* no. 2 (1997): 163-174. doi:10.2307/2539372 https://www.jstor.org/stable/2539372?seq=1#page_scan_tab_contents
Gene I. Rochlin & Chris C. Demchak (2008) The Gulf war: technological and organizational implications, Survival, 33:3, 260-273, DOI: 10.1080/00396339108442594
https://www.tandfonline.com/doi/abs/10.1080/00396339108442594?journalCode=tsur20

[38] United Nations. Security Council. "SECURITY COUNCIL REJECTS DEMAND FOR CESSATION OF USE OF FORCE AGAINST FEDERAL REPUBLIC OF YUGOSLAVIA." News release, March 26, 1999. https://www.un.org/press/en/1999/19990326.sc6659.html.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

the early 2000s, however, perceived incursions and transgressions would ultimately lead Russian policy-makers to regard the United States as unreliable and potentially undermining of its long-term goals. Some important factors that may have lead to these perceptions and results of them include the second Gulf War, United States support of regimes unfriendly to Russia in its near-abroad, and United States military basing in Central Asia. The second Gulf War likely contributed further to international perceptions of the United States as an unstable and arrogant actor because, like the bombing campaign during the Kosovo War, the second Gulf War was not endorsed by the United Nations.[39] The United States in the latter stages of the first decade of the 21st century was also quite openly supporting countries that challenged Russian primacy in its near-abroad. Examples of these would include Georgia and Ukraine, states that both would face Russian backlashes.[40] Lastly, with regards to military basing, a clear example of conflict between Russia and the United States can be found in Kyrgyzstan. Initially, the United States, as part of its Operation Enduring Freedom war on terrorism, was allowed to lease Manas Air Base, near Bishkek. However, following years of colder relations and a Russian push for primacy in its Near Abroad, the base was closed in 2014. This was the last base to be closed in Central Asia, and to many indicated a political shift in the region from the United States to Russia.[41]

As noted earlier, Russian assertiveness would increase over time and its methods of

[39]"Iraq War Illegal, Says Annan." BBC News. September 16, 2004. http://news.bbc.co.uk/2/hi/middle_east/3661134.stm.

[40] Kuzio, Taras. (2005). Russian Policy toward Ukraine during Elections. Demokratizatsiya: The Journal of Post-soviet Democratization. 13. 491-517. 10.3200/Demo.13.4.491-518 http://www.taraskuzio.com/International%20Relations_files/russia_elections_ukraine.pdf

Zunes, Stephen. "U.S. Role in Georgia Crisis." Foreign Policy in Focus. August 14, 2008. https://fpif.org/us_role_in_georgia_crisis/.

[41]Dzyubenko, Olga. "U.S. Vacates Base in Central Asia as Russia's Clout Rises." Reuters. June 3, 2014. https://www.reuters.com/article/us-kyrgyzstan-usa-manas/u-s-vacates-base-in-central-asia-as-russias-clout-rises-idUSKBN0EE1LH20140603.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

containing problematic regimes in its near abroad have become well known. In particular, actions in Ukraine and Crimea have shed light on its usage of Hybrid Warfare. Further, the 2016 United States presidential election has shown the lengths to which Russian operatives will go to attempt to manipulate public opinions through Information Warfare. While the United States is still the preeminent cyber power in the world, the Russian Federation has found its own ways to use technology to challenge United States hegemony. However, the United States and its policy-makers are now adapting to this new and challenging cyber environment. In particular, as noted earlier, the author will use aspects of Deterrence Theory to examine and analyze the current adaptations and what may be in store for the future.

First, taking United States actions from a Classical Deterrence perspective, Threats of Punishment and Denial by defense will be examined. Threats of Punishment will examine how United States capabilities may or may not be made public, how a new hierarchy of national response (also known as a deterrence ladder) may be used, and how attribution problems will be present whenever punishments are considered. Denial by defense will examine how the United States is investing in upgrading and hardening network infrastructure, embracing proper cyber hygiene, improving network resiliency, and improving surveillance and active defensive measures. All of these investments and research are ultimately being done to alter a simple cost/benefit equation with regards to engaging in clandestine hacking of United States networks. If the costs greatly outweigh the benefits, hostile operators will largely be dissuaded. Attribution problems and their importance to a stronger defensive posture will also be examined.

Broad Deterrence will also be examined with Entanglement and Normative Taboos.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Entanglement will examine perceptions of costs and benefits of actions and the rise of the Internet and how more and more dependency may prevent hostile actions on the internet. However, it will be noted that this dependency is not present in all relations. Normative Taboos will discuss reputational costs of illicit online actions, how target acquisitions may change over time, how the rules of law in cyberspace may develop, and how emerging multilateral norms may deter future conflicts.

### 3.1 Threats of Punishment

United States cyber policies will likely evolve most noticeably and quickly in terms of Classical Deterrence. Beginning with Threats of Punishment, there are clear examples of the United States taking this path to deter hostile cyber operations. These examples may be divided into two approaches, first, revealing or not revealing capabilities to the public, and secondly, developing and maintaining a new and clear hierarchy of national responses to aggression. However, because of the proactive nature of this approach, attribution problems will be inherent.

There are two examples that highlight the sophistication of United States Cyber operations. The first case would be that of the Stuxnet worm. The Stuxnet worm is an extremely advanced and malicious program that was designed to target Iranian nuclear facilities. Work on the worm began in 2005, and initial versions were found in 2007.[42] It was a joint operation between the United States and Israel, with an additional goal of preventing overt Israeli strikes that may have sparked further conflict. Stuxnet would also change over time, according to the desires of its creators. Initially, it was a slower acting worm that destroyed equipment in less obvious fashion. In 2009, it was modified to be much more aggressive. As a result of this, it was more quickly

[42] Slayton, 95



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

found out after abnormalities became impossible to ignore.[43] Further, the worm spread around the world, and in 2010 it was discovered and analyzed by a Belarusian cyber security firm. That same year, after months of research and analysis, Symantec published a report on the worm that would lead to further independent research.[44] Following these releases, Stuxnet became widely known, and its success in Iran ended.

Much has been written on Stuxnet and whether it indicates that Cyber will favor offensive actions or defensive postures. Additionally, there has been discussion of the cost effectiveness of the worm.[45] In this paper, the perceptions that have arisen as a result of Stuxnet are the most important aspect. Much of this importance is derived from the sheer technical scope of the worm itself. As noted in chapter two, Stuxnet made use of four separate zero-day and two stolen certificates that took advantage of local network vulnerabilities to spread the virus. This indicates two things. First, discovering multiple zero-day exploits signifies an extremely high level of expertise, especially when using so many of these exploits for one program. Zero-day exploits are some of the most valuable and sought after hacks in the world, with the United States National Security Agency budgeting $25 million to purchase them in 2013 alone.[46] Further, the Stuxnet worm made use of two stolen certificates, digital documents that allow programs to run on an operating system. These, like zero-day exploits, would be worth in the millions of dollars.[47] Secondly, the nature of the Stuxnet worm indicates it was an extremely focused attack. Other

[43] Ibid.
[44] Slayton, 96
Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." Wired. July 11, 2011. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.
[45] Slayton, 108
[46] Slayton, 100
[47] Ibid.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

authors have attempted to quantify how much it may have cost to develop and deploy the worm, with numbers reaching as high as hundreds of millions of dollars.[48] This high price was deemed acceptable when the target was only one nuclear facility in Iran. While Stuxnet has never been publicly acknowledged by the United States, the sophistication and damaging potential of it has likely shaped perceptions of United States cyber power and whether hostile cyber incursions are worth the cost when the target is capable of throwing massive amounts of resources behind bleeding edge retributive cyber operations.

More recently, the United States has been noted for using cyber tools to sabotage North Korean missile tests. Following increasing North Korean aggression and a frenzied schedule of ballistic tests, the Obama administration began exploring more methods to deter or destroy launches.[49] Some of these methods have been cyber based, such as using cyber operations to interfere with North Korean missile control systems; however, other proposed methods are more direct, such as using drones and aircraft to shoot down just launched missiles. The cyber approach, also known Left of Launch, was likely first used in 2014. It was during this period that a large number of the missiles failed at various stages of launch and flight. Over time launch records, however, improved. It is possible that the initial cyber attacks were found and dealt with, similar to Stuxnet. In 2017, missiles again began to fail and Kim Jong Un ordered an investigation into possible hacking through imported hardware and also had senior security officials executed in response.[50] It is possible that not all failed missile tests were due to cyber

[48] Slayton, 98

[49] Sanger, David E., and William J. Broad. "Trump Inherits a Secret Cyberwar Against North Korean Missiles." The New York Times. March 4, 2017. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

[50] Persio, Sofia Lotto. "NORTH KOREA EXECUTES OFFICIAL IN CHARGE OF NUCLEAR TEST SITE: REPORT." Newsweek. December 19, 2017. http://www.newsweek.com/north-korea-purges-and-executes-official- charge-nuclear-test-



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

attacks from the United States. There is a definite possibility that it was also a result of incompetence, bad luck, or compromised North Korean officials. However, it is highly likely, even assured when taking into account testimony on Korean targeted cyber attacks, that the United States and its cyber operatives and intelligence officers have been behind many of the failed launches.[51] While the primary importance of this subject would be regarding United States-North Korean relations, this story is also important in terms of cyber and threat perceptions. Where Russia, for example, is most famous for botnets and spam, the United States has illustrated capabilities that include sabotaging high security nuclear enrichment facilities in Iran and manipulating North Korean ballistic missile tests. Even when exposed, these operations may have value in deterring future cyber operations against the United States because of how sophisticated a response could be; as any reader of recent National Security Agency leaks would be amazed and horrified at the scope of their power. Further, many discussions on possible cyber programs are available in public records, although specific details are often omitted.[52] It would be quite simple for any foreign power to find hints at United States cyber power through these records, and to likely abstain from any harmful cyber actions.

With a clear perception of the United States as a sophisticated cyber operator, a well developed hierarchy of national responses to aggression would also serve to deter actions through threats of punishment. A ladder of possible responses to aggression may consist of:

site-report-752196.

[51]Patterson, Dan. "Cyberweapons Are Now in Play: From US Sabotage of a North Korean Missile Test to Hacked Emergency Sirens in Dallas." TechRepublic. https://www.techrepublic.com/article/cyberweapons-are-now-in-play- from-us-sabotage-of-a-north-korean-missile-test-to-hacked-emergency/.

[52]United States. The White House. Office of Management and Budget. By Mick Mulvaney. https://www.politico.com/f/?id=0000015f-931e-ded9-a15f-9bdf94370000.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

diplomatic, economic, cyber, physical force, and nuclear force.[53] Currently, all major powers acknowledge the possible damaging power of diplomatic, economic, physical, and nuclear responses. As public and leaked information on cyber capabilities come to light, the cyber aspect of the deterrence ladder will gain importance for foreign powers considering belligerent actions. However, it should be noted that in the hierarchy, cyber responses are in a mid-level position; nuclear weapons and regional force projection capabilities will continue to serve as the anchor of the deterrence ladder.

The United States has engaged in cutting edge advanced cyber attacks and these attacks have driven perceptions of the United States as a powerful cyber foe. As a result, many would-be attackers are likely put off from attacking the United States, for fear of overwhelming retaliation. Threats of punishment may serve as a useful tool to reduce cyber incursions; however, as a result of attribution issues it is limited. As noted earlier in chapter 2, attribution problems are particularly associated with retaliatory actions and, as will be discussed later, norms violations. Threats of punishment would likely serve as part of a comprehensive deterrence ladder, however, motivated advanced cyber operatives may not be dissuaded by threat perceptions alone.

### 3.2 Denial by Defense

While Threats of Punishment as deterrence to a large degree requires attribution to function, Denial by Defense has very little need for attribution to succeed.[54] This is because of the at times passive nature of this approach to deterrence. Denial by defense would involve several different approaches to change the cost/benefit analysis of potential aggressors. These

[53] Nye, 55
[54] Nye, 56



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

include hardening networks, improving general cyber hygiene, improving their resilience and capacity to recover, and improving general surveillance and the active defense of networks. All of these would increase the difficulty of attacking United States networks.

Hardening networks would be one of the most basic approaches to improving defenses, along with improving general cyber hygiene. Hardening networks would essentially be attempting to improve the impregnability of networks. One possible tactic would include protecting critical systems from data overload, a tactic often used by hackers to bring down websites through denial-of-service attacks.[55] Another option would be to increase usage of authentications to prevent outside access to sensitive data.[56] Lastly, a more active approach to hardening systems would involve constantly monitoring and patching systems.[57] This would require trained operators who understand what are normal system conditions, and who would be able to react quickly to possible threats. This final aspect would also be considered active defense. Hardening of defenses would likely reduce low-level incursions as it would greatly change the aggressors cost/benefit analysis.[58]

Another important approach to improving deterrence through defense would be by improving cyber hygiene. As discussed at length in Chapter two, many of the most spectacular hacks are as a result of simple user error. The Stuxnet worm, for example, was likely delivered into a closed network through an infected USB stick.[59] The possible Korean missile hacks were

[55] Mandel, Robert. *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*. Washington, DC: Georgetown University Press, 2017. 202.
[56] Mandel, 202
[57] Ibid.
[58] Nye, 56
[59] Zetter, Kim. "An Unprecedented Look at Stuxnet, The World's First Digital Weapon." Wired. November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

also likely a result of user error, as Kim Jong Un executed multiple security officials for either incompetence or possible treason. Improving in this regard would involve constant training and retraining of staff, ensuring that no one with access to sensitive data would unknowingly click on a Spear-Phishing email or enter data into false login pages. Cyber hygiene development for the United States government would involve the development of a set of best practices that require accountability from users. The United States, in response to the WannaCry virus and other hacks, passed legislation in 2017 that seeks to establish best practices when it comes to cyber hygiene.[60] While the Promoting Good Cyber Hygiene Act is not mandatory currently, it is likely that in the future these best practices will become standardized and expected; particularly the federal government and those wishing to do business with the federal government will be expected to follow the rules outlined in the Act.

Improving network resilience and their capacity to recover is another important way to improve deterrence through improved defensive measures. Network resiliency assumes that at some point the cyber attackers will prevail. However, if the attacked networks can quickly recover, there is a lowered incentive for an attack at all. Joseph Nye offers a clear example to explain how network resiliency may dissuade aggressive actions. In his example of resiliency, if Japan had known how resilient the United States would be following Pearl Harbor, it is likely that no attack would have occurred in the first place.[61] Developing resilience in the cyber world can take a multitude of forms. One approach could include developing redundancy in systems and redundancy in important infrastructures in case of attacks, however it would be quite

[60]Orrin Hatch United States Senator for Utah. "Hatch Introduces Legislation to Combat Cybercrime." News release, June 29, 2017. United States Senator Orrin Hatch. https://www.hatch.senate.gov/public/index.cfm/2017/6/hatch- introduces-legislation-to-combat-cybercrime.

[61] Nye, 56



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

expensive. Joseph Nye also offers cheaper examples of developing resiliency, such as continuing to train officers how to navigate by the stars; this would be in case global positioning systems were knocked out.

The United States government has already begun to improve resiliency, as the Department of Homeland Security and United States Computer Emergency Readiness Team offers a Cyber Resilience Review (CRR) service.[62] This method of analyzing and improving resiliency is done on a voluntary basis and has seen success with a wide variety of government and non-government customers, including the Department of Homeland Security, the Department of Energy, the United States Postal Service, and Lockheed Martin. The CRR service enabled a structured and repeatable plan of improving technical resiliency for those that opted into the service. However, it should be noted that CRR reports are considered classified, and even with a Freedom of Information Act request will not be released.

Lastly, the United States is improving the surveillance of its networks and developing a more active defensive posture to further deter aggressive actors. Active defense as a concept has changed over the past decades, as debates over how to respond to aggression in kind with inherent attribution issues were made. In 2017, Dorothy E. Denning and Bradley J. Strawser published an interesting article wherein they apply concepts of air defense to cyber defense.[63] The definitions of active and passive defense they use are as follows: "*Active cyber defense* is a direct defensive action taken to destroy, nullify, or reduce the effectiveness of cyber threats against friendly forces and assets, and *passive cyber defense* is all measures, other than active

[62]"Assessments: Cyber Resilience Review (CRR)." United States Computer Emergency Readiness Team. https://www.us-cert.gov/ccubedvp/assessments.

[63]Denning, Dorothy E., and Bradley J. Strawser. "Active Cyber Defense: Applying Air Defense to the Cyber Domain." In *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

cyber defense, taken to minimize the effectiveness of cyber threats against friendly forces and assets. Put another way, active defenses are direct actions taken against specific threats, while passive defenses focus more on protecting cyber assets from a variety of possible threats" (194-195).[64] Further, the pair ultimately argue that while there are ethical issues at times, similar to air defenses that may impose collateral damage, the ends may justify the means. The authors cite the case of the Coreflood botnet takedown as an example of using active defense effectively[65]. The Coreflood botnet was a Russian creation released in 2010. It infected millions of systems that included state and local government agencies, airports, defense contractors, banks, and financial institutions. The program would open a backdoor in the compromised computer and then gather what useful information it could find.

The active defensive measures had several steps and a grouping of the Federal Bureau of Investigation, Department of Justice, and the Internet Systems Consortium (ISC) worked together to bring down the Russian threat.[66] First, the ISC was given the legal go-ahead to switch its servers with Coreflood's command and control servers. The government was also allowed to take over domain names that were being used by Coreflood. When infected machines would then attempt to contact the command and control servers for instructions, they were issued stop orders. This neutralized the damaging effects of the malware on host machines. Following this action, the FBI would forward the IP addresses of infected machines to Internet Service Providers, who would then inform their customers. Microsoft also cooperated, by releasing an updated Software Removal tool to help victims remove the malicious code.

[64] Denning and Strawser 194-195
[65] Denning and Strawser 196
[66] Denning and Strawser 196-197



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

The authors draw an analogy between this case and defending against a hijacked aircraft, with hijackers receiving information from a separate command center. In the air defense case, the defenders would jam the command center and replace the signal with their own, ordering the hijackers to land at a specific airport. The specific airport would then be given identifying information so the hijackers could be apprehended on arrival. This approach provided by the authors would also be used by Microsoft, who commandeered the control servers of two Zeus botnets, preventing future harm.

The example above provides some specific means of using an active defense against intruders; the United States government has also taken it upon itself to fund and implement the proliferation of an active defense mindset throughout the country. In a similar fashion to the aforementioned Cyber Resilience Reviews, DARPA has developed new active defense technologies and the Department of Defense has been offering usage to interested parties.[67] The United States government has acknowledged the threats of the future, and is actively researching and funding ways to deter these threats.

Denial by defense has been an important deterrent since the internet and networking itself arose. The United States has adapted to new threats posed by nation-state and non-government actors by hardening networks, improving general cyber hygiene, improving network resilience and capacity to recover, and improving general surveillance and the active defense of networks. At the highest level of government, this aspect of deterrence has been embraced. As a result, many actors will likely be dissuaded at present and into the future.

[67]"Active Cyber Defense (ACD)." Information Assurance by the National Security Agency. https://www.iad.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

### 3.3 Entanglement

In addition to Classical Deterrence, Nye also looks to Glen Snyder's definition of deterrence and recalls Broad Deterrence to provide a framework in cyberspace. Entanglement is one of the methods of deterring hostile actions in cyber space. In particular, Nye mentions again how perceptions of costs and benefits will determine whether hostile actions are undertaken. As a result of the interdependencies that have developed in the international community, many states may find ties too deep to risk severing. Nye provides a possible example of entanglement preventing a Chinese cyber attack. In his example, Chinese operatives are dissuaded from attacking the United States power grid because the economic costs to China would be extreme.[68] The Chinese Communist Party in many ways relies on continued economic growth to maintain legitimacy, and much of this growth is now driven through the internet and trade with other large states, such as the United States. However, Nye also acknowledges that closed off nations, such as North Korea, would likely not be dissuaded by entanglement mechanisms because they are not deeply connected with other states, with the exception of China.[69]

British historian Nicholas Lambert draws analogies between the 19th and early 20th century and our current globalized world.[70] In the first age of globalization, there were attempts at waging what could be called the world's first version of cyber warfare. Undersea cables were connecting the world at the time, and financial markets were becoming more and more intertwined. In particular, grain prices became more similar around the world and would also react to news in far flung lands that previously had no bearing on domestic pricing. British

[68] Nye, 58
[69] Ibid.
[70] Lambert, Nicholas "Brits-Krieg: The Strategy of Economic Warfare." In *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

strategists of the time discussed and planned a manner of economic warfare that focused on attacking these rising interdependencies. The logic followed that because the United Kingdom was the hegemon of that period, any economic fall out stemming from this strategy would be less severe than that to befall its enemies. However, Lambert notes that as the world globalized, different interest groups became more powerful domestically.[71] As a result, matters of strategy would encompass many interest groups and these financial interest groups would not tolerate strategies that undermined their profits. The economic warfare strategy would only last for roughly three months before being abandoned.

This historical example has similarities to contemporary events as well, in particular with relations between the United States and China. Nye provides a 2009 example, wherein the People's Liberation Army urged the Chinese government to sell some of China's dollar reserves to punish the United States for arms sales to Taiwan. The Chinese Central Bank lobbied against this action, suggesting that such a tact would impose large costs on China. The result was the government siding with the Central Bank and not imposing measures against the United States.[72] These British and Chinese measures were also based on broader domestic fears. The British military planners of the day acknowledged that economic warfare would likely ruin the domestic economy in the blink of an eye; as a result, they were forced to consider stationing a large portion of the available army in large industrial cities to maintain order. Chinese government officials, with a preoccupation regarding mass movements and protests, would likely have the same fears if any actions were taken that negatively affected large swathes of the economy.

[71] Lambert, 143
[72] Nye, 58



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Further, Nye considers different perceptions between groups within a united state body and how they may change over time depending on their own interests. The example given is of Cyber within the Chinese PLA versus economic units within the Chinese government, and how both groups may perceive potential cyber war and its costs as different. Again, this calls to mind British events during the early 20th century, wherein domestic pressure groups urged strategists to call off their economic warfare plans. In the 21st century, many new actors have emerged in the technology field around the world, and their support is considered important by governments.

While economic interdependence did not prevent World War 1, strategies that potentially undermined the global trading system further were not undertaken due to British domestic pressures. Assuming the United States has a vested interest in systemic stability, and that many other nation-states share those interests, growing interdependence and entanglement arising as a result of the Internet is likely to dissuade aggressive state-sponsored actions that risk the economy. In addition, as financially oriented pressure groups gain in power, these disparate voices will further petition to prevent anything that may harm their bottom lines or general domestic stability; as were the cases in Britain and China. However, the effectiveness of entanglement relies on the underlying support of the Internet and the international systems by participating powers. Those that do not benefit from the status quo, or those that are controlled by interest groups that do not perceive the benefits of participation as outweighing the costs, will likely not be dissuaded from aggressive actions. An earlier example given was North Korea, that is largely shut off from global society. Further, when comparing Russian interests to those of China, it is likely that entanglement would be less of a factor affecting cost/benefit analysis of



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

cyber incursions for the Russian parties.

### 3.4 Normative Taboos

The last method of deterrence referenced by Nye is through norms and taboos. Initially, one can look to nuclear weapons and chemical and biological weapons as historical examples of weapons that have developed norms and taboos regarding usage. With regards to nuclear weapons, Nye notes how initially they were considered usable even in limited conflicts.[73] However, over time and after many treaties and agreements their usage has become restricted. Further, there are now clear taboos with regards to developing nuclear weapons programs as seen in global responses to Iranian and North Korean nuclear programs. With regards to chemical and biological weapons, he notes that they as well have undergone this process and are now restricted by international treaties and agreements. However, as a caveat, it is noted that some states will still pursue and use these taboo weapons. Syria and Iraq are offered as examples of offender states that have seen international responses due to their transgressions. Further, Nye notes that due to the image of these weapons, states risk reputational costs if it is found they are breaking norms and taboos. All of these separate examples provide a starting point when analyzing the United States and its development of norms and taboos in working to deter cyber attacks.

The United States has been working to develop cyber norms for the past several years. However, much of the language and style of development it wishes to use runs counter to those wished for by other powers, such as Russia and China. This mismatch culminated in 2017 at the conclusion of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. It was

[73] Nye, 60



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

there that the United States' efforts to codify cyber norms into international law was rejected.[74] However, while sweeping legal and norms developments failed there has been progress at a smaller scale. For example, in 2015 the United States and China agreed to not engage in economic cyber espionage.[75] These bilateral agreements may pave the way for future multilateral agreements and norms development. In addition, rather than undertaking system wide legal agreements, the United States has made norms development progress by voluntarily promoting non-legally binding codes of conduct. For example, the United States has supported the view that the internationally recognized laws of armed conflict (LOAC) should apply in cyberspace.[76] These laws prohibit deliberate attacks on civilians. In addition, the United States has supported a ban on targeting civilian facilities in peacetime. As Nye notes, this is not a pledge of no first use of cyber weapons, but rather is pledging to not use cyber weapons against civilians or civilian facilities in peacetime.[77] This more lax approach to norms building saw some success at the GGE in 2015, where that years report discussed reducing attacks on civilians rather than developing binding legal codes.[78] Although, as noted earlier, when more solid legally binding agreements

[74]U.S Department of State. Office of the Coordinator for Cyber Issues. "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security." News release, June 23, 2017. https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

Väljataga, Ann. "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly." NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. September 1, 2017. https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html.

[75]Nakashima, Ellen, and Steven Mufson. "U.S., China Vow Not to Engage in Economic Cyberespionage." The Washington Post. September 25, 2015. https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html?noredirect=on&utm_term=.87b9f0d10a53.

[76] Nye, 61

[77] Nye, 61

[78] United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015 http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

were suggested in 2017, certain parties balked. A reason for Russian and Chinese reluctance to embrace codified legal cyber developments is likely the inherent power of the United States in the cyber realm. If retaliatory measures and guidances were written into international law, this would make cyber espionage operations against the United States possibly much more costly. Further, United States written law would most certainly strategically favor United States interests.

If lower level norms development continues, future cyber attacks may become more and more taboo. In particular, cyber attacks that could be construed as violating sovereignty may be met with stiff consequences. In the United States case, following 2016 election manipulation, the Obama administration responded with sanctions against Russia. This will be helped as attribution technology improves, and as more victim countries cooperate to transparently acknowledge and respond to cyber incursions. An example of this transparency can be seen with responses to attacks from APT28: FancyBear. The hacking group, likely of Russian origin, has been associated with the 2016 United States election hacking, possibly hacking into the German defense and interior ministries in 2018, and hacking into multiple Olympic Games likely in response to Russian athlete doping bans.[79] Over time, governments, non-government organizations, and the press have become more sophisticated in their analysis and open about hacks. This has helped push a narrative of Russia as an aggressive cyber nation and the United

[79]Harding, Luke, and Alec Luhn. "Putin Says Russian Role in Election Hacking 'theoretically Possible'." The Guardian. June 1, 2017. https://www.theguardian.com/world/2017/jun/01/putin-says-russian-role-in-election-hacking-theoretically-possible.
Perper, Rosie. "Russian Hacking Group Fancy Bear May Have Spied on Germany's Government." BusinessInsider. February 28, 2018. http://www.businessinsider.com/russian-hackers-fancy-bear-germany-cyber-attack-2018-3.
Matsakis, Louise. "HACK BRIEF: RUSSIAN HACKERS RELEASE APPARENT IOC EMAILS IN WAKE OF OLYMPICS BAN." Wired. October 1, 2018. https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

States and other western countries as victims. In response, the United States and others have a precedent to respond to hacking with economic sanctions or through other means and offenders must deal with reputation costs in international society. Over time, these aggressive actions will likely become more and more taboo, and the cost/benefit analysis of cyber incursions will correspondingly change due to increased reputational costs.

The development of norms and taboos in cyberspace is still in flux. However, it should be noted that it took multiple decades for the first nuclear agreements to be signed, as well. The United States has approached deterrence through norms and taboo development by engaging in lower level bilateral agreements, by attempting to codify norms into international law, and by punishing transgressions in a systematic fashion. Development of norms and taboos has been aided by the more and more transparent responses to hacks and cooperation between governments, that aids in attribution and takes control of the narrative. Norms and Taboos are not currently as strong a deterrent as the conventional options discussed above; however, in the future they may gain in power.

### 3.5 Conclusion

The United States sees itself as a cyber hegemon due to a legacy of funding advanced research projects with the Cold War in mind. Now, it finds itself attempting to deter attackers in an environment that favors offense over defense. It is attempting to deter attackers through four means. Conventionally, the United States approaches deterrence through Threats of Punishment and Denial by Defense. The United States has shown to the world its cyber power and is developing a clear hierarchy of retaliation and responses to prevent cyber attacks, however



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

attribution issues hamstring the power of punishment alone as a deterrent. The United States is also developing its Denial by Defense capabilities by hardening networks, improving cyber hygiene, improving resilience and ability to recover, and embracing a concept of active defense that deals with threats as they develop. These approaches will directly alter a threat's cost/benefit analysis when attacking and likely dissuade many attacks in the future. Using aspects of Broad Deterrence, the United States is also embracing entanglement and Norms and Taboos to prevent hostile incursions. Entanglement is largely developed through supporting and developing the current international system. As a result, the United States has seen a reduction in Chinese cyber incursions because of economic interdependencies. Norms and Taboos are the final approach to deterrence, and the least mature. However, the United States has been promoting norms with regards to cyber space at the lowest and highest levels, although with mixed results. Where some actors such as Russia and China are potentially revisionist in their relations with international society, the United States is firmly supportive of the system it built and its approach to cyber deterrence is indicative of this approach.





DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

## Chapter 4 Russia

Russian approaches to Information Warfare and Cyber Operations have evolved together in an organic fashion over the past century. The contemporary Russian approaches culminated in the 2010s with its well-known Hybrid Warfare tactics used in its Near Abroad and the Middle East. While the Cyber Operations are often discussed, they cannot be detached from a larger paradigm of Information Warfare. Information Warfare could be defined as the attempts by an actor to gain competitive advantages over its opponents in terms of the use and management of information and communication technology. It it closely linked to propaganda and psychological operations, and other forms of political warfare. Information Warfare has occurred throughout history, being discussed in works as ancient and varied as Sun Tzu and Homer. In the 20th century, the Soviet Union was also infamous for its Information Operations and many of the same tactics used during the Cold War continue to this day. During the Cold War the Soviet Union intelligence services made use of Active Measures. Active Measures involved using various types of operations to influence the course of world events. These included manipulating media, producing propaganda, disinformation campaigns, counterfeiting official documents, establishing international front organizations, and others. Interestingly enough, attempting to manipulate elections would also fall under Active Measures, and this was allegedly attempted in cyberspace in 2016.[80] In 1992, Soviet KGB archivist Vasili Mitrokhin defected to the United Kingdom and brought along large quantities of personal writings and archives from his time on the job. These writings provided evidence of specific actions by Soviet Intelligence against the

[80]Kramer, Mark. "Policy Memos: The Soviet Roots of Meddling in U.S. Politics." PONARS Eurasia. January 2017. http://www.ponarseurasia.org/memo/soviet-roots-meddling-us-politics.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

United States that include attempting to stir up controversy regarding the John F. Kennedy assassination, attempting to manipulate the Civil Rights Movement and discrediting Martin Luther King Jr., attempting to further stoke racial tensions in the wake of the Civil Rights Movement and the assassination of Martin Luther King Jr., amongst others.[81] The archive notes also provide information on operations carried out internationally supporting communist regimes and various attempts at general espionage operations. Much of the logic of these Active Measures was based on using non-conventional means to defeat a conventionally more powerful opponent. However, during the Soviet Era much of this was also ideological in nature. Following the collapse of the Soviet Union, Information Warfare has continued unabated and the logic is the same. The ideological slant is missing or different now, and the focus is on protecting what is left of the Russia of today from those encroaching on its borders and attempting to weaken its sphere of influence.

Meanwhile, the Soviet Union was also experimenting with networking while ARPANET developed in the United States. The Soviet version was known as OGAS, and was developed by Victor Glushkov.[82] However, the goals for Soviet researchers were vastly different from their American counterparts. Where the American internet precursors were largely funded by the government and focused on helping improve military readiness and facilitating improved research and development between various campuses, the Soviet proposals and iterations were largely based on more efficiently allocating resources to improve central state planning of the

[81]Andrew, Christopher M. & Mitrokhin, Vasili. (1999). *The Mitrokhin archive : the KGB in Europe and the West*. London : Allen Lane 296-297, 298, 308-309, 310.

[82]Peters, Benjamin. "The Soviet InterNyet." Aeon. October 17, 2016. https://aeon.co/essays/how-the-soviets-invented-the-internet-and-why-it-didn-t-work.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

economy.[83] Ironically, the state-funding allowed ARPANET to develop and later lead to the development of the modern internet in the capitalist United States; in contrast, because of a desire to not upset the status quo and as a result of conflicts of interest within a complicated bureaucracy Soviet officials denied state funding to OGAS and other types of networking projects, strangling any possibilities of an indigenous internet developing.[84]

Without their own internet or computer development, the Soviet Union fell behind the West in this regard. This would continue until the breakup of the Soviet Union. Following the Soviet Union's collapse, the Russian Federation and former Soviet states would see the rise and proliferation of private Internet Service Providers. Former Soviet states were also allowed to connect to the internet proper in the early 1990s. User numbers would continue to increase into the 2000s, with Russia overtaking Germany in 2011 for number of unique internet users.[85] Future plans are to continue improving internet penetration and to improve quality as well; although, it should be noted that there is still a noticeable urban-rural divide in Russia with regards to internet access.[86]

As discussed earlier in Chapter 3, Russian-United States relations have gone through periods of varying degrees of amity during the 1990s and 2000s. It is this fraught relationship and the conventional power imbalances between the two states that has helped to foster the

[83]Peters, Benjamin. "The Soviet InterNyet." Aeon. October 17, 2016. https://aeon.co/essays/how-the-soviets-invented-the-internet-and-why-it-didn-t-work.

[84]Baraniuk, Chris. "Why the Forgotten Soviet Internet Was Doomed from the Start." BBC Future. October 26, 2016. http://www.bbc.com/future/story/20161026-why-the-forgotten-soviet-internet-was-doomed-from-the-start.

[85]ComScore. "ComScore Releases Overview of European Internet Usage in September 2011." News release, November 14, 2011. https://www.comscore.com/Insights/Press-Releases/2011/11/comScore-Releases-Overview-of-European-Internet-Usage-in-September-2011?cs_edgescape_cc=TW.

[86] Acılar, Ali & Markin, Maxim & Nazarbaeva, Elena. (2011). Exploring the Digital Divide: A Case of Russia and Turkey. 584.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

development of Cyber Operations as a key component of Russian Information Warfare strategies. In particular, the Russian Federation has found that asymetrical approaches to warfare and a renewed focus on Information campaigns in the cyber domain are effective when facing a stronger opponent that may seek to whittle away what remains of its sphere of influence. It is these approaches to cyber operations that have, as noted in Chapter 3, driven the United States to approach deterrence in the cyber realm in a more serious fashion. However, it is also possible to use similar metrics to examine Russian cyber development and how it developed and may continue to develop with regards to deterrence.

First, taking Russian developments from a Classical Deterrence perspective, Threats of Punishment and Denial by Defense will be examined. The Threats of Punishment section will first examine how Russian operatives have synthesized Cyber Operations with its concept of Information Warfare to punish perceived transgressions in its Near-Abroad, and how this display of offensive capabilities may be used to prevent further perceived transgressions and direct cyber attacks on Russian networks in the future. The Denial by Defense section will examine how the Russian Federation is now investing in network security for the future, and how in the past and in the present its networks are plagued by security issues.

Broad Deterrence will also be examined with Entanglement and Normative Taboos. Entanglement will examine how Russia's relations with its neighbors may alter cost/benefit analysis of cyber actions in its Near Abroad. Normative Taboos will examine official documents and responses to them in a similar fashion to Chapter 3, while also discussing how international reactions to certain Information and Cyber operations may alter Russian strategy in the future.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Ultimately, Chapter 4 will have a different tone from Chapter 3. This is because while the United States is looking to strengthen its position and maintain the international status quo that it helped build, the Russian Federation is continuing to focus on maintaining strength in its Near Abroad against incursions from materially more powerful adversaries. Where the United States enjoys its status as Cyber Hegemon, the Russian Federation and its strategies have developed because it holds no such status. As such, the approaches to deterrence and offensive information and cyber operations have become quite different between these two states.

**4.1 Threats of Punishment**

The Russian Federation, and Soviet Union, has throughout its history embraced asymetrical means to wage war. In the late 20th century and into the 21st, cyber means have appeared as a potent force allowing for a continuation of Information Warfare campaigns. Further, as relatively early adopters of this approach, the Russian Federation itself has had a first mover advantage when using cyber in an aggressive manner. This early approach allowed the Russian Federation to penetrate now antiquated attempts at conventional deterrence from NATO and the European Union to solidify Russian positions in the near abroad. There are examples of early cyber attacks in Estonia and Georgia, before the conflicts in Ukraine and Crimea that made Russia's Hybrid Warfare now infamous. All of these initial campaigns would, as mentioned in Chapter 3, provoke the United States and other western nations to revamp their approaches to cyber and network security in particular. Following alleged election hacking and influence campaigns in 2016, as well as after the Ukraine-Crimea conflict, western sanctions became common responses to aggressive Russian operations. Now, Russian operations have scaled back



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

slightly in terms of their overtness and cynicism; although, information operations are still occurring and occasional old-school tradecraft continues. Still, as a result of initial operations, there is likely reticence to now engage in cyber operations against Russia because of fears of reprisal. Similar to how United States deterrence has developed in this manner over time, Russian policy will likely begin to also develop in a similar fashion as cyber doctrines and policies emerge after a period of relative freedom and openness; freedom and openness that the Russian Federation took advantage of to engage more conventionally powerful powers with opposed interests through asymetric means. It is likely that the Russian Federation will share some developments with United States cyber policy in this category, particularly in regards to revealing or not revealing cyber capabilities to improve deterrence through threat of punishment. It remains to be seen if a clear response hierarchy will also develop, as is the case for the United States.

The initial campaign that called attention to Russia's growing cyber prowess were the 2007 Cyberattacks on Estonia. The Bronze Soldier of Tallinn is a Soviet Era war memorial located in Tallinn, Estonia. Political differences regarding interpretations of the monument and the events of the Second World War led to eventual plans to relocate the monument to be finalized in 2007. When news of the relocation became public, there was a massive backlash from ethnic-Russian Estonians and Russians abroad; there were demonstrations in Moscow and the Russian government suspended rail service to Estonia in response. In addition to two nights of rioting in the capital, known as Bronze Night, there were also large-scale cyber attacks on Estonian public and private websites and infrastructure. These attacks targeted the Estonian



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

parliament, banks, ministries, newspapers, and others; the most visible attacks were distributed denial of service (DDOS) attacks. This was an early iteration of modern Russian approaches to Cyber operations. On the ground at the time, the Estonian government was not sure how to respond. A Defense Ministry spokesman discussed the vexing nature of the attack, and what qualified as an act of war, in a phone call to the New York Times newspaper, saying "If you have a missile attack against, let's say, an airport, it is an act of war. If the same result is caused by computers, then how else do you describe that kind of attack?"[87]

What is most notable about this early iteration is the decentralized, almost crowdsourced, nature of the attacks. It has been suggested that officials in the Kremlin supported and helped to organize the Cyber-attacks, however, a large part of the operations were carried out by unaffiliated internet users attempting to mete out mob justice.[88] These internet users were compelled to act by an image of an affronted Russia; and Cyber-attack tools were provided through social media, on the then fledgling Russian language forums of the time. Relatively speaking, using botnets to carry out large-scale DDOS attacks is a simple task for even an amateur computer enthusiast. In fact, multiple United States security experts described the attacks as relatively insignificant in scale, from a technical standpoint.[89] The technology itself of the attacks was not notable, but rather the decentralized and deniable operations and the ability to scale up through use of local propaganda and patriotic Russians willing to defend their slighted

[87] Myers, Steven Lee. "*E-Stonia" Accuses Russia of Computer Attacks,* The New York Times, May, 2007 http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html

[88] Giles, Keir. "'Information Troops' – a Russian Cyber Command?"

[89] Waterman, Shaun. *Analysis: Who cyber smacked Estonia?,* United Press International, June, 2007 http://www.upi.com/Analysis-Who-cyber-smacked-Estonia/26831181580439/



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

homeland. Further, where major states such as the United States would view these methods as antiquated and insignificant in scale, as noted above; smaller states, like those directly bordering Russia, would likely find the threat of a Russian cyber operation quite compelling.

One year later, the 2008 Russo-Georgian War would be noted for being the first conflict that combined both cyber operations and conventional kinetic operations by the Russian Federation. This would further lay the foundation for the methods used to perfection in Ukraine. At the start of 2008, a diplomatic crisis was brewing between Russia and Georgia. There were many issues at hand, but most importantly, a pro-NATO president was making waves about pursuing membership for Georgia in the near future. The tinder for the conflict was Ossetian separatists shelling Georgian territory. In response, the Georgian military entered the conflict zone and quelled the separatists. On August 8th, after the Georgian's had engaged the Ossetian separatists, the Russian Federation commenced a combined arms assault on Georgian positions in the frontier regions and deep in Georgian sovereign territory. The reasoning was cited as being a humanitarian response to overt Georgian aggression towards South Ossetia and ethnic-Russian residents living within its borders.[90] In addition to defeating Georgian forces in the separatist Ossetian regions, the Russian forces also bombed important strategic points deep in Georgian territory and occupied Abkhazia, another breakaway region. After several days of frontier battling, the Georgian forces retreated, and on August 26th the Russian Federation recognized the independence of South Ossetia and Abkhazia. Even after the cease fire agreement, Russian forces still occupy South Ossetia and Abkhazia and agreements have been made to gradually

[90] Friedman, George. *The Medvedev Doctrine and American Strategy,* Stratfor Enterprises LLC., September, 2008 https://www.stratfor.com/weekly/medvedev_doctrine_and_american_strategy



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

integrate these territories militarily and economically into the Russia Federation. International opinion is divided regarding these regions, although the United States, the EU, and Japan, amongst others, recognize the regions as occupied territories.[91] Some analysts have described the Russian approach in Georgia, as well as in Ukraine, as "occupation without occupation."[92] This strategy allows Russian forces to maintain military outposts that threaten breakaway provinces, on the basis of humanitarian intervention, without fully committing military and political capital towards maintaining a legitimate occupation force in foreign territory. While Hybrid Warfare is the active approach, this long-term "occupation without occupation" cements the gains made during the initial incursions and allows Russia to pursue its geopolitical aims without crossing a red line and create uncertain conflicts in states that it wishes to remain supplicant.

While Russia waged a kinetic war in its Near Abroad, there was also a war waged through media and cyberspace. During the prosecution of the Russo-Georgian War, Russia embedded sympathetic journalists with its troops and played up the humanitarian angle of its intervention.[93] This appeal to ethnic-Russian nationalism would also be later used extensively in Ukraine. Journalists frequently would describe the Georgian's as an aggressive foreign military massacring ethnic-Russian civilians. Ethnic-Russian casualty numbers were quoted in the

[91] "Foreign Ministers' Joint Statement on Georgia" U.S Department of State, Office of the Spokesman. August, 2008 https://web.archive.org/web/20080831110250/http://www.america.gov/st/texttrans-english/2008/August/20080827152352xjsnommis0.9067346.html

[92] Dunn, Elizabeth Cullen and Michael S. Bobick, *AMERICAN ETHNOLOGIST*, Vol. 41, No. 3, 405, ISSN 0094- 0496, online ISSN 1548-1425. C 2014 by the American Anthropological Association. All rights reserved. DOI: 10.1111/amet.12086 https://static1.squarespace.com/static/55f7642be4b07229ccbb16e7/t/5665d74ba976af13731334c6/1449514 8274 98/Dunn_Bobick-2014-Empire+strikes+back_war%26occupation.pdf

[93] "Russia to provide $200 mln in urgent aid for S. Ossetia," Sputnik International. August, 2008 https://sputniknews.com/russia/20080811115961365/



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

thousands, although by the end of the war and years after the number has been revised and proven to be vastly lower than these initial claims.[94] Similar to the Ukrainians, the Georgians were cast as western pawns being used to aggressively impinge on Russian territory and state interests in the name of NATO enlargement and a spread of foreign liberal ideas. In addition, the Russian government and sympathetic networks, especially the well-known Russia Today, would actively attempt to contradict and criticize any western reporting on the conflict.[95] Using false figures and assertions of "Russophobia" and inherent bias in foreign media to call into question the integrity of any and all western reporting, Russians at home and abroad would cling more tightly to the narrative spun by the Russian state information apparatus.

This bolstered nationalism was also used in the cyber realm. The official Russian government line was that the Russian government itself was not behind any cyber-attacks on Georgia. Instead, it may have been interested individuals who felt compelled themselves to attack Georgian websites and infrastructure.[96] Reports indicate that the vast majority of attackers were indeed civilians.[97] However, there was an initial organization and development of hacking tools and strategies that were designed specifically for a Georgian campaign. These tools, along with comprehensive guides, were then distributed through social media to patriotic Russians at home and abroad. The attacks themselves were not particularly sophisticated, being largely

[94] "Up In Flames: Humanitarian Law Violations and Civilian Victims in the Conflict over South Ossetia" Human Rights Watch, January, 2009 https://www.hrw.org/report/2009/01/23/flames/humanitarian-law-violations-and-civilian-victims-conflict-over- south

[95] Holdsworth, Nick, *Russia claims media bias,* Variety, August, 2008 http://variety.com/2008/scene/news/russia-claims-media-bias-1117990468/

[96] Markoff, John, *Before the Gunfire, Cyberattacks,* The New York Times, August, 2008 http://www.nytimes.com/2008/08/13/technology/13cyber.html

[97] Blank, Stephen. "Cyber War and Information War a la Russe." In *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press. 89.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

website defacement and DDOS attacks. However, the hacking tools and methods provided were quite sophisticated and clearly required time for adequate development and planning.[98]

In addition, the targets of the attacks were all integral to any type of Georgian defense or international response. Initial targets included governments and news media websites. This left both the Georgian public and international observers in the dark with regards to the conflict. Following Russian gains on the ground, the attack list was expanded to include local banks, less essential government websites, business associations, more news websites, and others. The attacks began on a large scale shortly after initial Russian incursions, and ended shortly after official military operations had ended. This lends more weight to the notion that the Russian Government, particularly the FSB and GRU, designed the hacking tools and prepared for the attacks before distributing them to a decentralized civilian force of amateur hackers.[99] This crowdsourced approach to Cyber has been quite effective against smaller neighbors and has allowed Russia to maintain cyber superiority in its sphere of influence with ample plausible deniability. However, notably, this combined Information Warfare approach now also takes into account outside observers. By attacking local and even international media, such as the BBC and CNN, Russia can maintain confusion and an artificial "fog of war," preventing any quick responses from either the defending state, or more crucially, observing western powers with a stake in the region. This aspect, confusing and muddling the conflict, became a hallmark of a winning strategy that continued in Ukraine.

[98]Bumgarner, John and Scott Borg, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008" United States Cyber Consequences Unit, August, 2009, 4, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

[99]Carr, Jeff, "Project Grey Goose Phase II Report: The evolving state of cyber warfare" greylogic, March, 2009, 5 http://fserror.com/pdf/GreyGoose2.pdf



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

This period saw US-Russian relations continue to decline and, following the Great Recession, the BRICS were seen as having the potential to design a new world order opposed to a United States/Western-led vision. The grand strategy aspect of this is seen developing in Estonia and Georgia, before reaching a complete form in Ukraine. The information aspect of the Georgian war focused on reframing Russian actions as righteous and painting western governments and reporting as inherently biased and antagonistic towards Russian interests. As noted earlier, pushing propaganda is nothing new in Russia; but the new methods and taking advantage of new technology to achieve these information goals is novel. In particular, it could be suggested that as Russian grand strategy has developed information/cyber strategy has become an integral part of a combined arms approach to its expansionism. Now, with offensive hacking tools and strategies, Russian Information Warriors can ensure that the only information leaving and entering a conflict zone is supporting their narrative. This culminates in Ukraine, where opposition to NATO expansion and expansion of western liberal values into Russia's Near Abroad was the primary goal; hearkening back to the Brezhnev Doctrine. What is most intriguing, is how the Russian state is able to use new information technology to defeat NATO's strategy of deterrence and prevent further expansion into Ukraine.

In 2014, after months of Euromaidan protesting, Russia-leaning Viktor Yanukovych was removed from office. On his departure, unmarked Russian military forces annexed Crimea and also moved into Eastern Ukraine to aid separatist militias. While a large portion of Eastern Ukrainians are skeptical of the European Union and differ greatly from the more cosmopolitan Western Ukrainians that overwhelmingly supported Euromaidan protesting, this was still a clear



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

violation of Ukrainian national sovereignty on the part of the Russian Federation. It was also a successful gambit in terms of strategy; and cyber played a big part in the success. When Russian aggression began on the ground, it is reported it was also combined with DDOS attacks on Kiev, Poland, and European Union offices.[100] This Russian made "fog of war," combined with already positive sentiment in Crimea, allowed Russian special forces precious time to quickly take control of Crimea and establish positions and open communications with Eastern Ukrainian separatists. Western states had no clear picture of the ground situation and as such had no way to act with confidence. By the time accurate intelligence was available, the costs of deterrence, defending Ukraine, were too high and facts had already been established on the ground in Russia's favor. As James J. Wirtz puts it "they shifted the onus of escalation onto NATO... In a sense, they created a situation in which NATO leaders must choose between suffering a harsh strategic defeat (the eruption of war in Europe) and the accommodation of the Russian annexation of Crimea and ongoing pressure against Ukraine."[101] As NATO members clearly would not accept an open large-scale conflict with Russia over a non-member state, Russian policy-makers accurately predicted what a delay on intelligence would mean to NATO forces. The deterrence strategy of NATO, combined military action, was defeated by a Hybrid Warfare model that focused on increasing uncertainty through cyber attacks and information manipulation. Techniques developed in Estonia and Georgia were used in a more streamlined and advanced form, and tailored perfectly for the primary opponent, NATO.

[100]Wirtz, James J., "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy" *Cyber War in Perspective: Russian Aggression Against Ukraine*, (2015): 35. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf

[101]Ibid.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

The Ukrainian conflict was the last open and major affront to NATO and the EU to date, however, there have been continued Information operations and alleged Cyber operations. The most infamous have been long-term cyber-espionage operations designed to extract sensitive data and attempts at affecting elections and domestic politics in EU member states and the United States. Methods used to affect elections and domestic politics include funding far-right and far-left parties, publishing questionable reports in English-language Russian media, hacking election candidates, and generally painting the narrative of a corrupt western elite political class infringing on Russian sovereignty and pushing for a globalized world at the expense of ordinary citizens. So far the success has been mixed. There is more upheaval and rising populism in EU member states, especially the United Kingdom and Italy, however this is mostly due to domestic concerns beyond the scope of Russian interference. In the United States as well, a popular Democratic party view would be that Russian agents won the election for Donald Trump, a figure more sympathetic to Russian interests, through hacking and propaganda efforts targeting Hillary Clinton. However, this again would discount the state of American domestic politics and the other variables at play. While the operations in its Near Abroad has stabilized Russian borders and given a clear message to NATO, it has also exposed to the world the cynical and at times unsophisticated nature of Russian Cyber operations.

However, while Russian offensive cyber actions are now heavily studied and prepared for, they have also imbued Russian words and wants with more power than in the past. Specifically, one can compare the previous Russian campaigns and their cyber operations with those of the United States. Where the United States has exposed its advanced skills through the



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

development of Stuxnet and the various intelligence leaks indicating the reach of the National Security Agency and Central Intelligence Agency, the Russian Federation has illustrated its power through its populist approaches to cyber campaigns that were well synthesized with its information operations and its ability to combine cyber with kinetic on short notice. Further, it has shown its willingness to engage in cyber operations against any target it deems a threat, ranging from the United States to Estonia. These capabilities will likely not worry the United States or other major powers outside of specific espionage threats. Instead, they will likely keep Russia's close neighbors and would-be vassal states more compliant and less likely to engage in patriotic cyber attacks against Russia. In similar fashion to the United States, now that the actual punishments and physical attacks have occurred, Russia may now embrace the threat aspect to get its way in its near-abroad. However, Russia will not just be deterring errant cyber operations with its threatening stature, it will also be deterring its neighbors from drifting closer and closer to the European Union and NATO; as noted above, cyber has developed a place in the Grand Strategy of Russia.

**4.2 Denial by Defense**

The Russian federation is famous for its offensive cyber operations and its global usage of cyber in its information warfare campaigns. It is not nearly as famous for having cutting-edge network security, for good reason. Russia is instead known for its insecure and vulnerable networks, often as a result of widespread use of pirated software. This is, to a degree, a result of its Soviet legacy. In the past, Soviet officials did not embrace a domestic computer or software industry and instead imported and pirated what was needed. However, now the vulnerabilities



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

caused by this lack of foresight are becoming more and more clear. For example, recent global malware attacks have greatly harmed Russian networks because of these vulnerabilities. Further, as time goes on it is becoming more and more clear how poor network security and vulnerabilities are potentially a major threat to regime health and state interests. As a result, the Russian Federation is now more and more publishing and supporting doctrines that call for widespread reform in this area. Where in the past and in the present Russia is not known for a strong defensive posture, it is likely that better network security and denial by defense will be embraced to deter cyber threats. In similar fashion to Chapter 3, several aspects of Denial by Defense will be analyzed. These include hardening networks, improving cyber hygiene, improving resilience and capacity to recover, and improving general surveillance and the active defense of networks.

As noted earlier, Russian technology has developed in a very different fashion when compared to the United States and other western nations. This development path has important ramifications on how the Russian Federation approaches deterrence through Denial by Defense. Where the United States is now focusing on more advanced methods of denial, the Russian Federation is playing catch up throughout its society. One of the most important aspects to focus on for improving deterrence in the Russian Federation is simple cyber hygiene. As a result of its need to import hardware and software, it is common for Russian's to use pirated and outdated software. This habit and its dire consequences was made clear with the WannaCry virus in 2017.[102] The WannaCry virus, created thanks to earlier United States research and development

[102]Berry, Alex, Josh Homan, and Randi Eitzman. "WannaCry Malware Profile." FireEye. May 23, 2017. https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

noted in Chapter Two, infected roughly 300,000 computers worldwide, and 20 percent of those infections were in Russia. Even major state industries were affected, including the Russian Postal Service. This was largely a result of the usage of pirated and outdated software throughout Russia.[103] In response, Russian government officials urged private and government offices to update their software. However, because this software must be imported they are often much more expensive than the average citizen or small business can afford. It is possible to improve this aspect of deterrence quickly through better cyber hygiene practices; however, it would require specific and public measures, in similar fashion to those already taken by the United States as mentioned in Chapter Three. Further, if Russia's economy remains in a weak state, software piracy will likely continue if not increase.

While cyber hygiene is a major issue for improving Russian cyber security, the other aspects of Denial by Defense are also crucial and have been embraced by the highest levels of the Russian government. In 2016, a new doctrine on Information Security was published by the Russian Ministry of Foreign Affairs, and an unofficial english translation was provided.[104] The president approved doctrine provides an insight into how Russian officials view network security and how they may hope to improve and develop in the future. One interesting aspect of the doctrine is the continued emphasis on how the Russian Federation is currently besieged. This carries over into the cyber world, where the document notes that foreign powers are actively engaging in information operations against the Russian Federation, specifically targeting

[103]Stubbs, Jack. "Exclusive: Wannacry Hits Russian Postal Service, Exposes Wider Security Shortcomings." Reuters. May 24, 2017. https://www.reuters.com/article/us-cyber-attack-russia-idUSKBN18K26O.

[104]"Doctrine of Information Security of the Russian Federation." The Ministry of Foreign Affairs of the Russian Federation. December 5, 2016. http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

vulnerable Russian youth. The document also notes the dependence on imported hardware and software and a need to develop indigenous software and hardware, low levels of public awareness with regards to cyber hygiene, the need to improve resiliency and better harden networks, and it indicates a desire to engage international society to develop cyber norms. In contrast with the United States, there was little discussion of private industry and how the public and private space could cooperate to deter cyber attacks. These documents and tacit acknowledgment of Russia's cybersecurity weaknesses indicate that there may be more investment and an emphasis on improving denial capabilities. However, the document seems to focus on the Russian national interest and its armed forces with little attention paid to private actors. It is possible that as Russian state actors improve their denial capabilities, this will then leak over to the private sphere. Further, in contrast to the United States, actual advancements in defensive postures have not been widely publicized like in the United States. Therefore, it is difficult to evaluate the actual network security capabilities of the Russian Federation and its gradual improvements and projects with regards to the categories listed above. However, there are still official doctrines clearly indicating the desire for a strong emphasis on information security in the Russian Federation in the future. The result of these doctrines and their prescriptions would be consistent with the underlying arguments of this thesis, that states are shifting towards more defensive postures in cyberspace.

**4.3 Entanglement**

Where Classical Deterrence concepts are likely to be important in developing future cyber doctrines, Broad Deterrence concepts may not be as developed in the near or even distant



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

future with regards to the Russian Federation. This is because, in comparison to the United States and other great powers, the Russian Federation is much more at odds with the international status quo. Further, following successive rounds of sanctions the Russian Federation is less likely to care about economic ramifications for cyber actions when compared to the People's Republic of China. However, it is possible that aspects of Entanglement may be visible in a more subtle fashion over time. Specifically, Russia and its closest neighbors may refrain from destructive cyber campaigns because of the important bilateral economic and political ties that bind them. Although, the economic ties pale in comparison to those of the United States and China; so it is likely to not be as strong a factor for the Russian Federation.

One can look to Russia and its relations with states in its near-abroad when examining how entanglement may deter cyber attacks in the future. When analyzing Russian-Ukraine relations in particular, one can see that in spite of multiple years of violent conflict there are still large amounts of trade occurring between the two states.[105] While Ukraine and Russia continue to engage in violent physical conflict, trade continues, and Russia has not been hit by any widespread cyber attacks originating in Ukraine. The economic dependency of Ukraine on Russia could be a contributing factor that dissuades any cyber attacks, even when there is a frozen conflict in Eastern Ukraine. In similar fashion, Russian economic relations with Georgia have been improving as well as talks continue of new trade corridors.[106] It could be that Russian economic cooperation in its near abroad may dissuade cyber attacks by promoting dependency.

However, when compared to the United States, Russia's connections with nations outside

[105]Peterson, Nolan. "LONG AT WAR WITH EACH OTHER, UKRAINE AND RUSSIA TRADE ON." Newsweek. January 28, 2018. http://www.newsweek.com/long-war-each-other-ukraine-and-russia-trade-793142.

[106]Wayne, Shawn. "Russia–Georgia Trade Corridor Agreement Moving Forward." Georgia Today. May 25, 2018. http://georgiatoday.ge/news/10455/Russia–Georgia-Trade-Corridor-Agreement-Moving-Forward.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

of its near-abroad are much weaker. There are no analogs to the United States-China relationship to be found within the Russian Federation and its pool of neighbors. While Russia is able to ensure pliancy from its nearest neighbors, it has no such powers over those further afield. Specifically, Russia would likely not be able to dissuade, for example, the United States or China from engaging in aggressive cyber operations through economic entanglement alone. As noted in Chapter Three, because Russia does not support the international regime as wholeheartedly as other states, entanglement is much less likely to work in its favor in this regard. Where other Classical means of deterrence will likely adjust cost/benefit analyses of cyber incursions, entanglement alone is likely to hold little value in deterring actions from larger and more powerful states not on the immediate periphery of the Russian Federation.

**4.4 Normative Taboos**

Normative Taboos will likely, as mentioned in Chapter Three, ultimately hamstring Russia's usage of cyber operations as a way to counter more conventionally powerful foes. As noted, during formal discussions of regulating cyberspace Russia and China often balk at attempts at developing binding legal norms. This is because such measures would harm their abilities to compete with more conventionally powerful opponents such as the United States or NATO. However, as time passes and norms develop at a grassroots level, the Russian Federation will not be able to continue its behaviors without encountering rebuke. This could ultimately aid in Russian attempts at deterring cyber attacks on its own networks, as rival states themselves are dissuaded from attacks. However, Russia is not taking the lead in this regard and as noted earlier these developments will likely be the slowest to come about globally.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

As discussed in Chapter Three, the United States has been developing cyber norms over the past several years. These have ranged from small-scale bilateral talks to attempts at the United Nations to develop multilateral legally binding legislation. In contrast, the Russian Federation has not been as active in this regard as the United States. Or, to put it differently, Russia has not approached norms development in the same fashion as the United States. Where the United States would like a multilateral legally binding and comprehensive resolution with regards to cyber, the Russian Federation seems to prefer resolutions that emphasize national sovereignty as being of utmost importance. For example, where the United States would support international resolutions that ultimately lead to the ability to punish transgressions in cyberspace, Russia may view these supranational approaches as dangerous and potentially infringing on sovereignty. This is similar to China, although the PRC has been much more open to bilateral agreements with states such as the United States and Canada.

The Russian Federation is more likely to passively benefit from norms development than to be an active participant in their creation. For example, in the future, while it may be unwise to engage in cyber operations, the Russian Federation may instead enjoy an environment where incursions are reduced in frequency overall.

**4.5 Conclusion**

Russia has developed its internet infrastructure quickly and its ability to use cyber as part of its overarching Information Warfare paradigm has been impressive. With regards to deterrence and dissuasion, according to Joseph Nye's categorization, Russian policy differs from American policy as a result of inherent philosophical differences with regards to international



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

society and the status quo. However, in some areas there are overlaps, specifically with regards to Classical Deterrence. Threat of Punishment has developed in a fashion similar to the United States. The Russian Federation has consistently exposed its abilities in this area, and now this knowledge likely dissuades cyber incursions. Further, the at times risky nature of Russian operations may result in a stronger dissuasion factor because, unlike the United States, it could be implied that the Russian Federation would pay less mind to attribution problems or questions of legality and norms. Denial by Defense is also developing in a fashion similar to the United States, although in a much less advanced fashion. Interestingly, similar to the development of the internet in Russia as a whole, future problems could arise because of the too centralized nature of governance in Russia. Whereas in contrast, the decentralized nature of governance in the United States and the embrace of the private sector may allow for technology and cyber hygiene habits to develop more quickly. While methods of Classical Deterrence are clearly developing in the Russian Federation, the measures of Broad Deterrence are less apparent. Entanglement is difficult to measure or view as a serious factor because Russia finds itself at odds with the established status quo. Normative Taboos are also difficult to measure because of this similar outsider status, as well as a desire to prevent cyber from becoming too regulated too quickly; so as to prevent the reduction in Russian abilities to wage asymetric warfare through cyberspace. Ultimately, the Russian Federation is beginning to take cyber security seriously as evidenced by high level doctrines published by the Ministry of Foreign Affairs. Over time it is likely that these gradual shifts in policy will, in concert with developments from status quo powers such as the United States, lead to a more restrained and defensive focused Russian Federation in cyber



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

space.






DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

## Chapter 5 Conclusion

This thesis has attempted to analyze the United States and Russia with regards to deterrence in the cyber realm. More specifically, the argument has been made that Cyber operations will become less offensive and more regulated in nature over time. Recent work from Joseph Nye was used as an initial framework to analyze the respective states and their developments in this area. The thesis drew on deterrence theory, specifically Joseph Nye's approach to deterrence in the cyber realm. Chapter two provides more information on the history and context of deterrence theory in general, followed by analysis of Joseph Nye's attempts at bringing deterrence to the world of cyber. In this paper, deterrence is approached through four mechanisms: threat of punishment, denial by defense, entanglement, and normative taboos. Chapter two also provides a discussion on sources used in this thesis and a discussion on the more technical and difficult aspects related to researching and analyzing this subject.

Chapter three provides an analysis of the United States and its approaches to Cyber throughout the 20th and 21st century. Initially, there is a discussion of the history and context of the internet and cyber operations. Following this, each respective section of Nye's framework is analyzed with the United States in mind. Threats of punishment illustrates the United States taking steps to deter cyber incursions through revealing its own offensive capabilities and through the development of a clear hierarchy of responses to aggression. Denial by defense focuses on the investments that the United States is making in both the public and private sector to prevent cyber incursions. Both Classical Deterrence sections also discuss the problems of attribution in cyberspace. Entanglement discusses the trade ties that the internet has fostered and



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

provides examples of how these have prevented conflict between the United States and China. Normative Taboos discusses the bilateral agreements emerging as well as attempts at developing multilateral agreements at the United Nations. However, it is noted that this category is likely the least developed currently and will be the slowest to develop in the future. This section provides ample evidence that the United States is officially approaching cyber deterrence seriously; and the results will likely be seen in the near-future due to its status in international society.

Chapter four provides and analysis of the Russian Federation and its approaches to Cyber throughout the 20th and 21st century. Initially, there is a discussion on the history of the internet in Russia and the Soviet Union; as well as a discussion on the concept of Information Warfare. Special note is paid to the concept of Information Warfare and Active Measures, and how cyber is considered part of a larger Information Warfare paradigm. Following this, each respective section of Nye's framework is analyzed with the Russian Federation in mind. The Threats of Punishment section examines how Russian operatives have synthesized Cyber Operations with the Russian concept of Information Warfare to punish perceived transgressions in its Near-Abroad, and how this display of offensive capabilities may be used to prevent further perceived transgressions and direct cyber attacks on Russian networks in the future. The Denial by Defense section examines how the Russian Federation is now investing in network security for the future, and how in the past and in the present its networks are plagued by security issues. Entanglement examines how Russia's relations with its neighbors may alter cost/benefit analysis of cyber actions in its Near Abroad. Normative Taboos examines official documents and responses to them in a similar fashion to Chapter 3, while also discussing how international reactions to



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

certain Information and Cyber operations may alter Russian strategy in the future. This chapter differs markedly from Chapter 3, because where the United States is a hegemonic and status-quo power the Russian Federation is approaching operations from the perspective of a nation under siege attempting to regain power and status in the international community. As such, the mechanisms of Classical Deterrence are much more visible than those of Broad Deterrence. It is argued that the Russian Federation is clearly investing in developing its network security capabilities and has top-level interest in cyber security, although this is more notable in the physical realm rather than that of norms and taboos.

### 5.1 Recommendations for Future Research

Recommendations for future research include expanding the amount of states studied. Specifically, adding additional great powers would provide insight on how states are developing their own individual doctrines and approaches to cyber security; although, it is also noted that expanding the depth of this study would go beyond the scope of a Thesis. Further recommendations would include more technically oriented interviews with network security experts, working in the public or private sector, to further bridge the gap between the hard and soft sciences. Additionally, direct interviews with military officials, American and Russian, would provide great insight into how cyber security is developing and how doctrines are being followed. However, as noted in chapter two, due to the sensitive nature of this topic it is likely that whatever information was gleaned from said interviews would be of questionable utility.

### 5.2 Suggested Topics for Future Research

1. North Korean and South Korean approaches to deterrence



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

2. Chinese and Indian approaches to deterrence
3. How deeply criminal Russian elements augment official cyber operations
4. How Russia, and other states, approach cyber deterrence with regards to countries in their near-abroad and with those further afield
5. Research on how Russian approaches to Information Warfare and Active Measures have or have not changed with the advent of cyber operations
6. How Active Measures, and specifically cyber propaganda efforts, are used by other states in their near-abroad (Specific subjects could include Taiwan and the PRC)
7. How the United States is approaching Russian Information Warfare efforts in the cyber realm and adjusting policies, and how they compare and contrast with past policy adjustments from during the Cold War

How the fracturing of the internet, for example the Great Firewall and North Korea's closed off network, may impact cyber deterrence

**5.3 Final Thoughts and Discussion**

Currently, as noted in the first chapter, analysts are preoccupied with the power and further potential of offensive cyber operations. Defensive posturing is often regarded as bordering on impossible due to the multitude of factors working against the defender. Specifically, attribution problems are consistently noted as a key aspect that will befuddle network security specialists into the future. With no ability to react to cyber incursions in a timely and accurate manner, it is quite clear that cyber attackers are in an advantageous position. However, the aim of this thesis is to delve deeper into this problem by analyzing past cases and



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

seeing how trends may or may not alter this offensive advantage in the future.

Joseph Nye's framework provides a great guide for this task; in particular, his approach to deterrence with regards to cost/benefit analysis and dissuasion allows for much more realistic thinking on this issue. When approaching cyber operations from this cost/benefit analysis standpoint, the idea of an emerging defensive paradigm seems more and more likely. As has been illustrated, both the United States and the Russian Federation are attempting to make strides with regards to their defense postures and deterrence and dissuasion capabilities. The United States, because of its status-quo position, has evidence that lines up with all of Joseph Nye's noted methods of deterrence and dissuasion. In contrast, the Russian Federation heavily leans towards using Classical methods of deterrence and pays less attention to Broad methods. Regardless, both are at times attempting to change the offensively focused nature of the current world of cyber operations.

It remains to be seen whether these approaches will lead to fundamental change in the future, as much also rests on the advancement of attribution technology. Regardless, there is ample evidence that nation-states throughout the world will eventually embrace defensive posturing and possibly also norms development that may lead cyber to develop in a similar trajectory to nuclear weapons; where their destructive capabilities are viewed as too grave to leave to chance. Initially in this paper, cyber was also compared to the emergence of air power in the 20th century. Air power changed the nature of warfare and how strategy was designed; in the present, cyber is actively changing the nature of warfare and developing doctrines and paradigms as well. It remains to be seen exactly how states and their doctrines adjust to these new threats;



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

although like air power, it is likely that defensive countermeasures will emerge in time as status-quo powers prefer norms development and defensive posturing.





DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

**Bibliography**

Acılar, Ali & Markin, Maxim & Nazarbaeva, Elena. (2011). Exploring the Digital Divide: A Case of Russia and Turkey. 584.

"Active Cyber Defense (ACD)." Information Assurance by the National Security Agency. https://www.iad.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm.

"Advanced Persistent Threat Groups." FireEye. Accessed March 27, 2018. https://www.fireeye.com/current-threats/apt-groups.html.

Andrew, Christopher M.& Mitrokhin, Vasili. (1999). *The Mitrokhin archive : the KGB in Europe and the West*. London : Allen Lane 296-297, 298, 308-309, 310.

Applegate, Scott D. "The Dawn of Kinetic Cyber." Presented at the 5th International Conference on Cyber Conflict, Tallin, Estonia, 2013. https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf

APT28—A Window Into Russia's Cyber Espionage Operations?. Special Report. FireEye, 2014. https://www2.fireeye.com/apt28.html.

Baylon, Caroline, Roger Brunt, and David Livingstone. "Cyber Security at Civil Nuclear Facilities: Understanding the Risk." Chatham House. 2015.

"Assessments: Cyber Resilience Review (CRR)." United States Computer Emergency Readiness Team. https://www.us-cert.gov/ccubedvp/assessments.

Baraniuk, Chris. "Why the Forgotten Soviet Internet Was Doomed from the Start." BBC Future. October 26, 2016.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

http://www.bbc.com/future/story/20161026-why-the-forgotten-soviet-internet-was-doomed-from-the-start.

Berry, Alex, Josh Homan, and Randi Eitzman. "WannaCry Malware Profile." FireEye. May 23, 2017.

https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html.

Biddle, Stephen. “The Gulf War Debate Redux: Why Skill and Technology Are the Right Answer.” *International Security 22,* no. 2 (1997): 163-174. doi:10.2307/2539372

https://www.jstor.org/stable/2539372?seq=1#page_scan_tab_contents

Blank, Stephen. "Cyber War and Information War a la Russe." In *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press. 89.

Buchan, Russell. “The International Legal Regulation of State-Sponsored Cyber Espionage.” In *International Cyber Norms: Legal, policy & Industry Perspectives* edited by Anna-Maria Osula and Henry Rõigas, 65-86. Tallinn: NATO CCD COE Publication, 2016.

Bumgarner, John and Scott Borg, “Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008” United States Cyber Consequences Unit, August, 2009, 4, http://www.registan.net/wp- content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

Carr, Jeff, “Project Grey Goose Phase II Report: The evolving state of cyber warfare” greylogic, March, 2009, 5

http://fserror.com/pdf/GreyGoose2.pdf

Clarke, Richard A. and Robert K. Knake. Cyber War: The Next Threat to National



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Security and What To Do About It. New York, NY: Ecco, 2010: 6

Clayton, Blake and Adam Segal. “Addressing Cyber Threats to Oil and Gas Suppliers.” Council on Foreign Relations. 2013.

ComScore. "ComScore Releases Overview of European Internet Usage in September 2011." News release, November 14, 2011. https://www.comscore.com/Insights/Press-Releases/2011/11/comScore-Releases-Overview-of-European-Internet-Usage-in-September-2011?cs_edgescape_cc=TW.

Cordesman, Anthony H. with the assistance of Charles Ayers. *Korean Special, Asymetric, and Paramilitary Forces*. Washington, DC: Center for Strategic and International Studies, 2016. 29. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160809_Korean_Special_Asymmetric_Paramilitary_Forces.pdf

Demchak, Chris C. and Peter J. Dombrowski. “Rise of a Cybered Westphalian Age”. *Strategic Studies Quarterly*, (Spring 2011): 31-62.

Denning, Dorothy E., and Bradley J. Strawser. "Active Cyber Defense: Applying Air Defense to the Cyber Domain." In *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press.

"Doctrine of Information Security of the Russian Federation." The Ministry of Foreign Affairs of the Russian Federation. December 5, 2016 http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Dunn, Elizabeth Cullen and Michael S. Bobick, *AMERICAN ETHNOLOGIST*, Vol. 41, No. 3, 405, ISSN 0094- 0496, online ISSN 1548-1425. C 2014 by the American Anthropological Association. All rights reserved. DOI: 10.1111/amet.12086 https://static1.squarespace.com/static/55f7642be4b07229ccbb16e7/t/5665d74ba976af1373 1334c6/14495148274 9 8/Dunn_Bobick-2014-Empire+strikes+back_war%26occupation.pdf

Dzyubenko, Olga. "U.S. Vacates Base in Central Asia as Russia's Clout Rises." Reuters. June 3, 2014. https://www.reuters.com/article/us-kyrgyzstan-usa-manas/u-s-vacates-base-in-central-asia-as-russias-clout- rises-idUSKBN0EE1LH20140603.

Fahrenkrug, David T. "Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy." Presented at the 4th International Conference on Cyber Conflict, Tallinn, Estonia, 2013. https://ccdcoe.org/cycon/2012/proceedings/fahrenkrug.pdf

"Foreign Ministers' Joint Statement on Georgia" U.S Department of State, Office of the Spokesman. August, 2008 https://web.archive.org/web/20080831110250/http://www.america.gov/st/texttrans-english/2008/August/20080827152352xjsnommis0.9067346.html

Friedman, George. *The Medvedev Doctrine and American Strategy,* Stratfor Enterprises LLC., September, 2008 https://www.stratfor.com/weekly/medvedev_doctrine_and_american_strategy



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Geist, Edward. “Deterrence Stability in the Cyber Age.” *Strategic Studies Quarterly,* (Winter 2015): 44-62.

Gellman, Barton, and Ashkan Soltani. "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." *Washington Post*, October 30, 2013. Accessed March 24, 2018. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.12576195b082.

Giles, Keir. “’Information Troops’ – a Russian Cyber Command?” Presented at the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011. http://conflictstudies.org.uk/files/Russian_Cyber_Command.pdf

Giles, Keir, “Russia’s Public Stance on Cyberspace Issues,” presented at the 4th International Conference on Cyber Conflict, Tallinn: Cooperative Cyber Defense Centre of Excellence (2012): 63-74, https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf

HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group. Special Report. FireEye, 2015. https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf

Harding, Luke, and Alec Luhn. "Putin Says Russian Role in Election Hacking 'theoretically Possible'." The Guardian. June 1, 2017.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

https://www.theguardian.com/world/2017/jun/01/putin-says-russian-role-in-election-hacking-theoretically-possible.

Harold, Scott W. "The U.S.-China Cyber Agreement: A Good First Step." *The Rand Blog* (blog), August 1, 2016. Accessed March 26, 2018. https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html.

Hathaway, Oona A. "The Drawbacks and Dangers of Active Defense." Presented at the 6th International Conference on Cyber Conflict, Tallinn, Estonia, 2014.

Heickerö, Roland. (2018). FOI Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.

Holdsworth, Nick, *Russia claims media bias,* Variety, August, 2008 http://variety.com/2008/scene/news/russia-claims-media-bias-1117990468/

"Iraq War Illegal, Says Annan." BBC News. September 16, 2004. http://news.bbc.co.uk/2/hi/middle_east/3661134.stm.

Junio, Timothy J. "How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate." *Journal of Strategic Studies,* (2013).

Kramer, Mark. "Policy Memos: The Soviet Roots of Meddling in U.S. Politics." PONARS Eurasia. January 2017. http://www.ponarseurasia.org/memo/soviet-roots-meddling- us-politics.

Kristensen, Hans M., Norris, Robert S., and Ivan Oelrich. "From Counterforce to Minimal Deterrence: A New Nuclear Policy on the Path Toward Eliminating Nuclear Weapons."



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Federation of American Scientists and The Natural Resources Defense Council. Occasional Paper No. 7. April 2009. https://fas.org/pubs/_docs/occasionalpaper7.pdf

Kuzio, Taras. (2005). Russian Policy toward Ukraine during Elections. Demokratizatsiya: The Journal of Post-soviet Democratization. 13. 491-517. 10.3200/Demo.13.4.491-518 http://www.taraskuzio.com/International%20Relations_files/russia_elections_ukraine.pdf

Lambert, Nicholas. "Brits-Krieg: The Strategy of Economic Warfare." In *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press.

Libicki, Martin C., Lillian Ablon, Timm Webb. "The Defender's Dilemma: Charting a Course Toward Cybersecurity." RAND Corporation. 2016.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* Vol. 22, Issue 3 (2013): 365-404.

Lotrionte, Catherine. "A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence." *Georgetown Journal of International Affairs* Special Cyber Issue, 3rd ed. (January 2014): 71-84. http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13007_Lotrionte-CYBER-III.pdf

Mandel, Robert. *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks*. Washington, DC: Georgetown University Press, 2017.

Markoff, John, *Before the Gunfire, Cyberattacks,* The New York Times, August, 2008 http://www.nytimes.com/2008/08/13/technology/13cyber.html



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Matsakis, Louise. "HACK BRIEF: RUSSIAN HACKERS RELEASE APPARENT IOC EMAILS IN WAKE OF OLYMPICS BAN." Wired. October 1, 2018. https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/.

Medvedev, Sergei A. "Offense-Defense Theory Analysis of Russian Cyber Capability." Master's Thesis, Naval Postgraduate School, 2015. http://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf?sequence=1

Myers, Steven Lee. "*E-Stonia" Accuses Russia of Computer Attacks,* The New York Times, May, 2007 http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html

Nakashima, Ellen, and Craig Timberg. "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did." *Washington Post*, May 16, 2017. Accessed March 24, 2018. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.4ec69cfa3812.

Nakashima, Ellen, and Steven Mufson. "U.S., China Vow Not to Engage in Economic Cyberespionage." The Washington Post. September 25, 2015.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html?noredirect=on&utm_term=.87b9f0d10a53.

Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* Vol. 41 Issue 3 (Winter 2016/17): 44-71.

Orrin Hatch United States Senator for Utah. "Hatch Introduces Legislation to Combat Cybercrime." News release, June 29, 2017. United States Senator Orrin Hatch. https://www.hatch.senate.gov/public/index.cfm/2017/6/hatch-introduces-legislation-to-combat-cybercrime.

Patterson, Dan. "Cyberweapons Are Now in Play: From US Sabotage of a North Korean Missile Test to Hacked Emergency Sirens in Dallas." TechRepublic. https://www.techrepublic.com/article/cyberweapons-are-now-in-play-from-us-sabotage-of-a-north-korean-missile-test-to-hacked-emergency/.

“Paul Baran and the Origins of the Internet.” Rand Corporation. https://www.rand.org/about/history/baran.list.html

Perper, Rosie. "Russian Hacking Group Fancy Bear May Have Spied on Germany's Government." BusinessInsider. February 28, 2018. http://www.businessinsider.com/russian-hackers-fancy-bear-germany-cyber-attack-2018-3



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

Persio, Sofia Lotto. "North Korea Executes Official In Charge of Nuclear Test Site: Report." Newsweek. December 19, 2017. http://www.newsweek.com/north-korea-purges-and-executes-official-charge-nuclear-test-site-report-752196.

Peters, Benjamin. "The Soviet InterNyet." Aeon. October 17, 2016. https://aeon.co/essays/how-the-soviets-invented-the-internet-and-why-it-didn-t-work.

Peterson, Nolan. "Long at War With Each Other, Ukraine and Russia Trade On.." Newsweek. January 28, 2018. http://www.newsweek.com/long-war-each-other-ukraine-and-russia-trade-793142.

Rivera, Jason, and Forrest Hare. "The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures." Presented at the 6th International Conference on Cyber Conflict, Tallinn, Estonia

Rochlin, Gene I. & Chris C. Demchak (2008) The Gulf war: technological and organizational implications, Survival, 33:3, 260-273, DOI: 10.1080/00396339108442594 https://www.tandfonline.com/doi/abs/10.1080/00396339108442594?%20journalCode=tsur20

Roigas, Henry "The Ukraine Crisis as a Test for Proposed Cyber Norms." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, 135-144. Tallinn: NATO CCD COE Publication, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Roigas_15.pdf

"Russia to provide $200 mln in urgent aid for S. Ossetia," Sputnik International. August, 2008



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

https://sputniknews.com/russia/20080811115961365/

Sanger, David E., and William J. Broad. "Trump Inherits a Secret Cyberwar Against North Korean Missiles." The New York Times. March 4, 2017. https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

Schelling, Thomas C. *Arms and Influence*. Yale University Press, 1966. http://www.jstor.org/stable/j.ctt5vm52s.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. doi:10.1017/CBO9781139169288.

Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. doi:10.1017/9781316822524.

Slayton, Rebecca. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* Vol. 41 Issue 3 (Winter 2016/17): 72-109.

Stubbs, Jack. "Exclusive: Wannacry Hits Russian Postal Service, Exposes Wider Security Shortcomings." Reuters. May 24, 2017. https://www.reuters.com/article/us-cyber-attack-russia-idUSKBN18K26O.

United Nations. Security Council. "Security Council Rejects Demand For Cessation of Use of Force Against Federal Republic of Yugoslavia." News release, March 26, 1999. https://www.un.org/press/en/1999/19990326.sc6659.html.

United States. The White House. Office of Management and Budget. By Mick Mulvaney.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

https://www.politico.com/f/?id=0000015f-931e-ded9-a15f-9bdf94370000.

“Up In Flames: Humanitarian Law Violations and Civilian Victims in the Conflict over South Ossetia” Human Rights Watch, January, 2009 https://www.hrw.org/report/2009/01/23/flames/humanitarian-law-violations-and-civilian-victims-conflict-over-south.

"U.S. Cyber Command (USCYBERCOM)." United States Strategic Command. September 30, 2016. Accessed March 27, 2018. http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber%20command-uscybercom/.

U.S Department of State. Office of the Coordinator for Cyber Issues. "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security." News release, June 23, 2017. https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

Väljataga, Ann. "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly." NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. September 1, 2017. https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html.

Virilio, Paulo. "The Kosovo War Took Place in Orbital Space." Interview by John Armitage. CTheory. October 18, 2000 Accessed March 26, 2018.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

http://www.ctheory.net/articles.aspx?id=132.

Waterman, Shaun. *Analysis: Who cyber smacked Estonia?,* United Press International, June, 2007

http://www.upi.com/Analysis-Who-cyber-smacked-Estonia/26831181580439/

Wayne, Shawn. "Russia–Georgia Trade Corridor Agreement Moving Forward." Georgia Today. May 25, 2018.

http://georgiatoday.ge/news/10455/Russia–Georgia-Trade-Corridor-Agreement-Moving-Forward.

Weedon, Jen. "Beyond 'Cyber War'" Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, 67-78. Tallinn: NATO CCD COE Publication, 2015.

Wirtz, James J. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, 29-38. Tallinn: NATO CCD COE Publication, 2015.

https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf

Zetter, Kim. "An Unprecedented Look at Stuxnet, The World's First Digital Weapon." Wired. November 3, 2014.

https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." Wired. July 11, 2011.



DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06

https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

Zunes, Stephen. "U.S. Role in Georgia Crisis." Foreign Policy in Focus. August 14, 2008. https://fpif.org/us_role_in_georgia_crisis/.






DOI:10.6814/THE.NCCU.IMPIS.010.2018.A06