2021

Hacking for peace: the case for cyber coercion

BOSTON UNIVERSITY

GRADUATE SCHOOL OF ARTS AND SCIENCES

Dissertation

HACKING FOR PEACE:

THE CASE FOR CYBER COERCION

by

TARA A. KEMMER

B.A., Boston University, 2002
A.M., University of Chicago, 2005

Submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

2021

Approved by

First Reader

Thomas Berger, Ph.D.
Professor of International Relations

Second Reader

Rosella Cappella Zielinski, Ph.D.
Associate Professor of Political Science

Third Reader

Kaija Schilde, Ph.D.
Associate Professor of International Relations

Fourth Reader

Jack Weinstein, Lieutenant General, USAF, Ret.
Professor of the Practice of International Security

HACKING FOR PEACE:

THE CASE FOR CYBER COERCION

TARA A. KEMMER

Boston University Graduate School of Arts and Sciences, 2021

Major Professor: Thomas Berger, Professor of International Relations

ABSTRACT

Are cyber capabilities a useful method for coercive diplomacy? If so, what conditions favor successful cyber coercion to produce a desired victim response? This research explores how cyber coercion can be used as a tool of statecraft to change an adversary's behavior and examines two cases over three temporal values. Examining the two cases of North Korea versus Sony and Russia versus Estonia illustrates practical lessons about the constraints and abilities of the employment of cyber coercion as well as how victim responses operate on a spectrum and can change over time.

In examining George's seven factors that favor coercive diplomacy and applying them to these cases, this research reveals four additional factors that ought to be included when addressing the dynamics that contribute to a victim changing their behavior in response to cyber coercion. The difference between a low-level attack (e.g. web defacement) compared with a high-level attack (e.g. paralyzing backbone servers) communicates two vastly different levels of threat to a victim and incurs extremely different costs for the victim. These technical aspects of cyber statecraft and their ramifications for cyber coercion are not covered by George's earlier works on coercive diplomacy, as few people in the 1990s were even considering cyber as a threat landscape.

This research does not provide one generalizable theory of how to conduct cyber coercion; rather, it provides a Utilitarian theory that identifies additional factors that favor cyber coercion and contributes to a *conditional* generalization. Further, it introduces the idea of examining this change in behavior *over time* to properly assess the impact of cyber coercion on the totality of the victim's behavior. Extending the time intervals reveals additional critical data necessary to fully analyze the nature of a cyber coercion dyad. Finally, it provides a hybrid method to attain attribution by fusing social science methodology with cybersecurity techniques. Together, this data and method serve to correct the conventional wisdom on two influential cases; this research traces the process that proves why a correction for each case is warranted; and, it shows how the choices an aggressor makes in its cyber coercive strategy can result in different outcomes for the victims.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ARPA	Advanced Research Project Agency
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CNO	Computer Network Operations
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
GGE	Groups of Governmental Experts
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IP	Internet Protocol
IR	International Relations
IT	Information technology
ITU	International Telecommunications Union
NATO	North Atlantic Treaty Organization
OEWG	Open-Ended Working Group
RMA	Revolution in Military Affairs
SPE	Sony Pictures Entertainment
SQL	Structured Query Language
SRI	Stanford Research Institute

TCP	Transmission Control Protocol
UCLA	University of California at Los Angeles
UCSB	University of California at Santa Barbara

CHAPTER 1. INTRODUCTION

"With cyberweapons, a war theoretically could be waged without casualties or political risk, so their attractiveness is great -- maybe so irresistible that nations are tempted to use them before such aggression is justified."[1]

"In comparison to the nuclear revolution in military affairs, strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950. Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy."[2]

Thucydides teaches us that the strong may dominate the weak and that power projection can result in victory in conflict, but that naked aggression and poor strategy can also backfire horribly.[3] "[I]n asymmetric conflicts the strong actor should almost always win"[4] but at times, the comparably weaker actor prevails. With the advent of cyberspace, and the associated vulnerabilities and audience costs it presents, weaker states have the ability to successfully engage in cyber coercion.[5] The potential for

---

[1] Lin, Patrick, Fritz Allhoff, and Neil Rowe. "Is It Possible to Wage a Just Cyberwar?" *The Atlantic Monthly*, June 5, 2012. Found at http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106 and accessed September 4, 2013.

[2] Nye Jr., Joseph. ""Nuclear Lessons for Cybersecurity?" *Strategic Studies Quarterly*, Winter 2011. p.19.

[3] Strassler, Robert B. and Richard Crawley. 1998. *The Landmark Thucydides: a Comprehensive Guide to the Peloponnesian War*. New York: Simon & Schuster. Specifically, compare the difference in the results for Athens versus Melos and Athens versus Sicily. In the Siege of Melos the Athenian power projection and Athen's rejection of the moral and just arguments from the Melians resulted in annihilation for the Melians. Conversely, the Athenian Sicilian Expedition, was a monumental disaster for the Athenians that resulted in lasting damage and foretold the eventual downfall of Athens.

[4] Arreguin-Toft, Ivan. "How the Weak Win Wars: A Theory of Asymmetric Conflict." *International Security,* Vol. 26, No. 1. Summer 2001. p. 96

[5] Political realism contains three key elements: (1) states exist in an anarchical system; (2) all

leveling of the playing field in what some call a "Fifth Dimension of Warfare,"[6] the cyber realm, changes the relationship between adversaries of unequal power. Cyber coercion introduces the opportunity for limited offensive cyber capabilities to be used also as a below-the-level-of-armed-conflict tool of statecraft in crisis and non-crisis situations. Cyber coercion provides another avenue for competition between adversaries, augmenting more traditional options like economic sanctions and other nonviolent activities. Here, the stronger power does not necessarily prevail. In looking at two cases of state's use of cyber capabilities for coercion, one state versus state, Russia against Estonia, and one state versus a non-state actor, North Korea against Sony Pictures Entertainment, this research examines what factors contribute to a victim's response to an aggressor's use of cyberspace.

The conventional wisdom on the impact of cyber statecraft, also referred to as information and communication technologies (ICTs),[7] on international relations, largely falls into two bipolar camps that began nearly thirty years ago: pessimists and optimists. The first wave pessimists believe "an electronic Pearl Harbor is waiting to happen," as Winn Schwartau, a pioneering cybersecurity expert, warned in testimony before Congress

---

states have a capacity to harm one another; and (3) states seek to increase their relative power to deter other states from attacking and/or to compel other states into making concessions. This is why Realists expect states naturally to exercise cyber statecraft options.

[6] Remarks as delivered by Gen. Ronald R. Fogleman, Air Force Chief of Staff, to the Armed Forces Communications-Electronics Association, Washington, April 25, 1995. Located at: http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm and accessed on June 1, 2018. See also "Cyberwar: War in the fifth domain." *The Economist*, June 1, 2010.

[7] While the term "cyber" in the United States has a broad, encompassing definition of all actions in cyberspace, the United Nations and the European Union use the term information and communication technologies (ICTs) to refer to cyber activities. For purposes of this paper, the term "cyber" will be the prevailing usage, but ICT may be employed when using references and quotations from European and United Nations sources.

in 1991.[8] Similarly, an early and influential study of the issue published by RAND in 1993 proclaimed "Cyberwar Is Coming!"[9] It is the central tenet of this camp that cyber represents a fundamental transformation in warfare. Alternatively, the second camp, the optimists, consists of those who believe that cyber capabilities are simply another weapon to be used alongside conventional military action. This second wave believes that cyber does not represent a watershed moment in the conduct of warfare and coalesces around the question, "...how authentic can a war be when things don't blow up?"[10] This research seeks to contribute to a burgeoning third wave of literature[11] by providing a Utilitarian theory that seeks to stake out an intermediate position, one that demonstrates utility of cyber statecraft while realistically providing parameters for its degrees of effectiveness as a tool of statecraft.

What is coercion and how does it apply to cyber statecraft? The figure below shows the components of cyber statecraft. To start with definitions, cyberspace is the

[8] Schwartau, Winn. Testimony at Hearing before the Subcommittee on Technology and Competitiveness of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, First Session, June 27, 1991, page 2. Located at: https://winnschwartau.com/wp-content/uploads/2019/06/Testimoney-1991-Computer-security_hearing.pdf and accessed on December 5, 2019.

[9] Cyberwar Is Coming!" John Arquilla and David Ronfeldt RAND Corporation analysts

[10] Stein, Jeff. "Book review: 'Cyber War' by Richard Clarke." *The Washington Post,* May 23, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/05/21/AR2010052101860.html

[11] Third wave scholars include: Timothy J. Junio. "How Probable is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate." *Journal of Strategic Studies*, 2013. 36:1, 125-133; ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Washington DC: Cyber Conflict Studies Association, 2013; Smeets, Max. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly*, Vol. 12, No. 3 (FALL 2018), pp. 90-113; and, Slayton, Rebecca. "What is the Cyber Offense-Defense Balance?" *International Security* 41:3. Winter 2016/2017. p. 72-109

terrain; cyber capabilities or cyberweapons are the means; cyberattacks are the method,[12] and cyber coercion-to-cyber warfare is the spectrum of activity that describes increased tensions occurring in cyberspace. The red box in Figure 1. below illustrates Schelling's definition of coercion, which consists of two forms: active coercion which is defined as compellence, and passive coercion defined as deterrence.[13] As he notes:

> Deterrence and compellence differ in a number of respects, most of them corresponding to something like the difference between statics and dynamics. Deterrence involves setting the stage—by announcement, by rigging the trip-wire, by incurring the obligation—and *waiting*. The overt act is up to the opponent. The stage-setting can often be nonintrusive, nonhostile, nonprovocative. The act that is intrusive, hostile, or provocative is usually the one to be deterred; the deterrent threat only changes the consequences *if the* act in question—the one to be deterred—is then taken. Compellence, in contrast, usually involves *initiating* an action (or an irrevocable commitment to action) that can cease, or become harmless, only if the opponent responds. The overt act, the first step, is up to the side that makes the compellent threat. To deter, one digs in, or lays a minefield, and waits—in the interest of inaction. To compel, one gets up enough momentum (figuratively, but sometimes literally) to make the other *act* to avoid collision. …Deterrence tends to be indefinite in its timing. …Compellence has to be definite.[14]

For George, coercion is employing "rational persuasion and accommodation as well as coercive threats to encourage the adversary to either comply with the demands or to work out an acceptable compromise."[15] It also "needs to be distinguished from

---

[12] According to Herb Lin, et al, "cyberattack refers to actions—perhaps taken over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks." Cited in William A. Owens, Kenneth W. Dam and Herbert S. Lin, eds., 'Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.' Washington, DC: The National Academies Press, 2009. p. 19.

[13] Schelling, Thomas. *Arms and Influence.* New Haven: Yale University Press, 1966. p. 70-72.

[14] Schelling, Thomas. *Arms and Influence.* New Haven: Yale University Press, 1966. p. 71-72.

[15] George, Alexander L. and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994. p. 7.

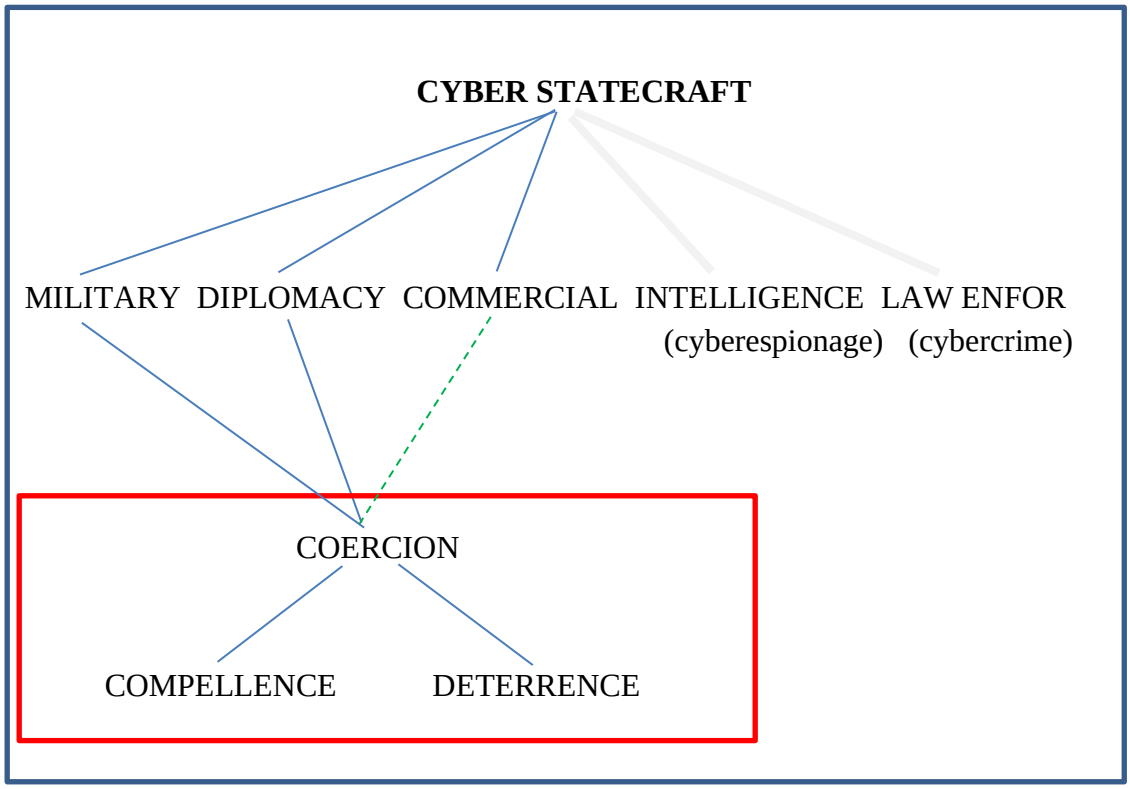
deterrence, a strategy that employs threats to dissuade an adversary from undertaking a damaging action not yet initiated.[16] When applied to cyber statecraft, George's definition artificially limits research by excluding deterrence. In a field where, less than ten years ago, a scholar noted that "no comparable comprehensive assessment of the impact of cyber warfare capabilities exists. Outside the slowly emerging policy literature there is limited scholarly work on the topic, leaving important theoretical questions unexamined,"[17] Schelling's more expansive definition including deterrence is more apt. Since cyber coercion can also cause secondary deterrence effects, as will be discussed later in this research, this research chooses to use Schelling's broader definition, while relying on George for his identification of the conditions that favor coercive diplomacy.

A visual representation of how Schelling's definition of coercion fits into cyber statecraft is depicted in Figure 1. As shown, cyber statecraft touches various realms to include military, diplomacy, commercial industry, intelligence and law enforcement. This research is bounded to the military, diplomatic and commercial spaces, as shown by the blue lines, and does not address intelligence and law enforcement, which is cyber espionage and cybercrime, respectively, and is illustrated by grey lines. Within the bounds of this research, a state may choose to use the military or diplomatic government entities to conduct cyber coercion, or the state may choose/may allow a commercial or private industry to conduct cyber coercion (as referenced in Jason Healey's Spectrum of

[16] Ibid.
[17] Liff, Adam. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." Journal of Strategic Studies, Vol. 35, No. 3, 401–428, June 2012. p. 402.

State Responsibility).

Figure 1. Cyber Statecraft



This research will show the following: 1) that cyber coercion can have significant impact on a victim's behavior, either positive or negative, when measured over time, more so than has been recognized in the literature thus far, and certainly of sufficient magnitude to warrant a serious reconsideration of the optimistic assessments of some analysts and scholars (i.e. the Second Wave literature). And, 2) cyber coercion is complicated, and while it offers some advantages for a would-be coercer, an expanded range of conditions must be met to favor successful coercion beyond those that must be

met to allow for success for more conventional forms of coercion as described by George's seven criteria.

Research Question: Importance for Academia and Policy Makers

Are cyber capabilities a useful method for coercive diplomacy? Under what conditions can cyber coercion be employed to produce a desired victim response? Are there conditions that are ripe for cyber coercion as opposed to economic sanctions or diplomatic moral arguments and threats? Should states and non-state actors invest in creating cyber capabilities or do they fail to compel or deter victims? Should weak, small or regional powers invest in cyber capabilities, or should they put their limited resources toward becoming a nuclear power or increasing air or sea power? Does cyber offer a level of power projection that a state could not otherwise exercise? Or does the utility of employing cyber tactics only have a cost-benefit when it focuses on other aspects like cybercrime?

Research thus far on the coercive effectiveness of cyber exploitation in relations among states has been focused largely in two camps: the pessimists and the optimists. The pessimists, in the first wave, emphasize assessing the value of cyber in the conduct of war-making, viewing it as revolutionizing how states conduct warfare and claiming it will cause widespread destruction. The optimists, on the other hand, representing the second wave, claim that cyber threats are exaggerated, that cyber conflict is unlikely to result in lethal violence and therefore it is little more than a nuisance.[18] "To constitute cyber warfare an action must be a potentially lethal, instrumental and political act of

[18] Gartzke, E. The Myth of Cyberwar. *International Security*, Vol. 38, No. 2, Fall 2013, p. 41–73. Liff, A. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35(3): 401-428, 2012. Rid, T. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35(1): 5-32, 2012.

force, conducted through the use of software."[19]

Each of these cohorts, the pessimists and the optimists, provides useful perspectives on the strategic nature of employing cyber capabilities, but each camp is too extreme and fails to see the middle road where cyber capabilities can be an effective and efficient method of statecraft. This dissertation raises a new set of questions and offers a deeper examination that provides a theoretical framework for effectively addressing the arguments of both the pessimists and optimists with respect to the usefulness of employing cyber coercion against soft, countervalue targets to gain a desired response from a victim as part of a state's strategy. Further, it will identify and examine what factors influence certain victim outcomes and how the coercive use of cyber capabilities can impose costs that are less than lethal but greater than mere nuisance.

Several actions in the cyber realm are below the level of armed conflict during peacetime, similar to economic sanctions, but like all aggressive actions and tools of coercive diplomacy, in cyber statecraft there exists the potential to increase tension and instigate armed conflict.[20] Cyber statecraft spans the spectrum of options from peacetime diplomacy to tension to crisis or even to outright war-making and provides a cyber

---

[19] Rid, Thomas. "Cyberwar May Not Happen." Located on the author's website at: https://ridt.co/wp-content/uploads/2011/10/Rid-KCL-comment.pdf and accessed on June 3, 2021.

[20] On May 5, 2019, the Israeli Defense Forces tweeted from its official, verified account: "We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed." This was watershed moment in the history of cyber aggression because it was the first time a kinetic strike was employed solely in response to a cyberattack in real-time against the hackers, but of course this action must be viewed within the larger construct of the Israeli-Palestinian conflict. The IDF tweet can be viewed here: https://twitter.com/IDF/status/1125066395010699264.

capability to supplement or supplant each method to solving conflict. Further, this study will discuss the likely implications for this use in practical policy applications. This interdisciplinary approach, drawing from the fields of political science and cybersecurity and computer operations, will improve our understanding of the coercion dynamic in the cyber realm and how the introduction of new technologies can be used effectively by states in the international system for political means.

The Study of Cyber Coercion

Successful coercion is hard, but not impossible. "In any crisis, the policy maker must decide *what* combination of persuasion, coercion, and accommodation to employ *and in what* sequence."[21] George helpfully reminds us of the goal in studying coercive diplomacy, namely:

> "The systematic comparison we undertake is not intended to formulate a sweeping set of generalizations that purport to explain in a simple way why coercive diplomacy sometimes succeeds and at other times fails. The phenomena of coercive diplomacy is too complex and the conditions and variables at play too numerous to permit formulation of such generalizations. …This will call…for *conditional* generalizations that identify those factors and variables noted in our case studies that, if present, favor the success of the strategy."[22]

There are ample examples in modern political literature of failed coercion using conventional arms threats and the reasoning for the failures ranging from misinterpreting

[21] George, Alexander and William E. Simons, eds. *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994. p. 277.
[22] George, Alexander L. and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994. p. 268.

reputation costs to poor target choice and execution.[23] In the cyber domain, with the added factors of secrecy and attribution complications, successful coercion can be even more difficult to achieve, but it is still possible.

In cyber coercion it is imperative to understand that each cyber dyad is unique, that they are motivated by different factors and that these differences can be leveraged in the course of a coercive act. A successful strategy for cyber coercion will require an adversary-specific approach. This approach includes understanding the different motivations and particular variables in a dyadic game to effectively use cyber as a tool to achieve a strategic objective. "Coercive diplomacy is a *flexible* strategy that is highly *context-dependent*;"[24]. as opposed to other types of coercion, cyber coercion has the added factor of mystery. In cyberspace, one is unable to see an aggressor's armory to calculate the extent of the hurt they might endure when threatened, and one may not even know their networks have been breached until they are confronted with the threat. Coercion can occur before the use of the force, through the use of force, or via a combination of diplomacy and force, with scholars disagreeing among these three

[23] Examples are included in the following: Sechser, Todd "Goliath's Curse: Coercive Threats and Asymmetric Power, *International Organization* 64, no. 4, October 2010: p. 627–60; Robert Pape, *Bombing to Win: Air Power and Coercion in War*. Cornell University Press, 1996. George, Alexander. *Forceful Persuasion.* Washington, DC, United States Institute of Peace Publisher, 1991. p. 77; Alexander L. George and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994; and Byman, D and M Waxman. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might.* UK: Cambridge University Press, RAND, 2002.

[24] George, Alexander. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. Washington, DC: United States Institute of Peace Press, 1991. p. 76-81. See also Alexander L. George and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994. p. 291.

definitions[25]. For purposes of this study, we will use the broad definition that encompasses all three options.

Bratton divides coercion into four main categories, the type of threat, the role of force, the actors and the definition of success, in Tables 1-4 below represents these distinctions as well as identifies the authors in the literature who concur:[26]

What types of threats are involved in coercion?	**Authors who concur**
Only compellent threats (i.e., coercion is different from deterrence)	Alexander George, Janice Gross Stein, Robert Pape
Both compellent and deterrent threats	Thomas Schelling, Daniel Ellsberg, Wallace Thies, Lawrence Freedman, Daniel Byman, and Matthew Waxman

Table 1. Types of Threats[27]

What role does force play in coercion?	**Authors who concur**
Coercion *before* the use of force (i.e. coercive threats made through diplomacy)	George, Gross Stein
Coercion only *through* force	Pape
Coercion through diplomacy *and* force	Schelling, Thies

Table 2 Role of Force[28]

[25] Bratton, P. "When is coercion successful? And why can't we agree on it?" *Naval War College Review*, 58 (3). p. 103.
[26] Ibid. p. 103.
[27] Ibid p. 100.
[28] Ibid. p. 103.

Who are the actors?	Authors who concur
Best thought of as identical, unitary, rational calculating actors	Schelling, George, Pape, and Daniel Drezner
Rational actors can be somewhat different (democracies vs. authoritarian governments) or are made up of a few simple parts (govt, military, public, etc.)	Pape, Risa Brooks, Byman and Waxman
Complex governments that both threaten and respond to threats differently[29]	Thies, David Auerswald

Table 3. Actors[30]

How is success defined?	Authors who concur
Full compliance with coercer's demands, independent of any other factors	Pape
Need to distinguish degrees of success. Possible to have partial success or secure secondary objectives without securing primary objectives	Kimberly Elliot, Drezner, Karl Mueller, and Byman and Waxman

Table 4. Definition of Success[31]

[29] Bratton uses the term "complex governments" to refer to regimes where regime composition and internal political struggles play a significant role and cannot be considered a "rational, calculating actor." He notes: "the coercer needs to know the 'political realities within the target state's government and to shape their policies in a way that maximizes the influence of those in the target state's government whose hopes and fears are most compatible with the coercer's objectives.' In some cases there will be factions that are compatible with the coercer's desires, in others not." In Bratton, P. "When is coercion successful? And why can't we agree on it?" *Naval War College Review*, 58 (3). p. 111.

[30] Bratton, P. "When is coercion successful? And why can't we agree on it?" *Naval War College Review*, 58 (3). p. 108. Pape sees the target as a unitary rational actor, but in *Bombing to Win*, he also notes differences in the reaction in the cases of Japan and Germany in WWII.

[31] Ibid. 111.

As noted, for purposes of this study, a broad definition modeled on Schelling that includes both compellence and deterrence will be employed in designing the coercion framework. Schelling notes, "the threat that compels rather than deters often requires that the punishment be administered *until* the other acts, rather than *if* he acts.[32]

Beyond the definition of coercion, there is the concept of cyber coercion. For purposes of this research, cyber coercion is defined as the "threat (implied or explicit) or limited use of [computer network operations] CNO to motivate a change in behavior by another actor that may involve cyber operations on their own or in conjunction with other coercive actions."[33] For purposes of this study, we will use the terms "computer network operations (CNO)," which is the modern definition, often used interchangeably with "cyber operations," and refers broadly to any activity taking place via computer networks.[34] Key questions in the application of coercive measures in the cyber realm include:

1. Under what conditions does cyber coercion produce particular victim responses on a spectrum from total acquiescence to complete refusal, or a combination in between?

[32] Schelling, Thomas. *Arms and Influence.* New Haven: Yale University Press, 1966.
[33] Hodgson, Quentin, Logan Ma, Krystyna Marcinek and Karen Schwindt. "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace." Santa Monica, CA: RAND. 2019. Located at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2961/RAND_RR2961.pdf
[34] For a primer on computer networks, please see Kurose, J. F. and K. W. Ross. Computer Networking: A Top-Down Approach, 5th Edition. New York: Addison Wesley, 2010.

2. For successful cyber coercion, is there a difference in following our tradition to counterforce and discriminate in targeting to focus on military targets, or is it more fruitful to focus on soft, countervalue (including non-military government) or targets?
3. How does cyber coercion and victim response change over time?

Cyber Coercion Conventional Wisdom

Cyberspace actions are commonly defined as operations that disrupt, deny, destroy, or degrade access to some networked asset. Strategic analysis of the cyber realm has experienced three waves: the alarmist/pessimist first wave, the silencing/optimist second wave, and now the pragmatist/utilitarian third wave. The principal inquiry at the core of this research is a multi-case qualitative examination of the conditions under which cyberspace provides an avenue for coercive diplomacy; the purpose of this analysis is two-fold: both theory-building and hypothesis testing.[35]

Is cyber coercion sufficient to yield a particular response from a victim and, if so, how? The conventional wisdom largely consists of two polarized camps that each approach the question of cyber coercive effectiveness as a binary option, instead of degrees of responses, while also ignoring temporal considerations, resulting in insufficient theoretical explanation. This research provides a middle-of-the-road theory, the Utilitarian theory, as a more plausible explanation for what factors determine the

[35] The methodology used to support this study will be extensively covered in the Research Design section in Chapter two.

spectrum of victim responses to using cyber coercion to achieve one's political goals. The additional factors this research identifies are 1) financial costs for the victim, 2) audience costs for the victim, 3) leadership destabilization potential through targeting of leadership, and 4) the amount of pressure on leadership.

Borrowing from the economic sanctions literature, the concept of degrees of success, or partial success, can be applied to cyber coercion and allow greater illumination of the factors contributing to the outcome of these cyber coercive actions. Additionally, introducing a temporal scale, combined with the degrees of effectiveness, results in richer descriptive and theoretical explanatory power. For this research, the determination of the degrees of effectiveness of cyber coercion encompasses a spectrum of changes in victim behavior that can translate to partial success to full success and partial failure to complete failure for the aggressor. This determination is also dependent on behavior change over time, factors which are excluded from the two sides of conventional wisdom on this subject.

The conduct of cyber coercion is not a fire-and-forget process. Cyber coercion is most often an iterative process; with the dynamics of an unfolding process, a state's initial cyber coercion strategy may adjust as hostilities continue. Both aggressor and victim may learn and adapt as a cyber coercive action progresses which is why examining changing temporal values are necessary to include in a comprehensive theory of cyber coercion. As George noted, the most important factor influencing success or failure in

coercion is the adversary's *perception* of each of these conditions.[36] If an initial strategy does not satisfy most or all of George's seven principles favoring coercive diplomacy (which are the factors whose presence or absence can contribute to the success or failure of a coercive strategy), we would expect to see the state adjusting its cyber coercive approach as the situation develops.

When applied to the case studies, the choices the aggressors, Russia and North Korea, made with respect to George's seven factors influencing successful coercive diplomacy are revealed, but they do not fully explain the divergent outcomes observed in the two dyads. Therefore, the identification of additional variables to explain the outcome for each case study is necessary.

[36] George, Alexander. *Forceful Persuasion.* Washington, DC, United States Institute of Peace Publisher, 1991. p. 81.

First, Second and Third Wave Literature

This research is focused on expanding the third wave scholarship, but I will begin by expanding on the first (cyber hysteric) and second (cyber skeptic) waves that were briefly described above. The two main cohorts weighing in on the value of cyber in international relations are diametrically opposed. One group believes that the presence of cyber represents a fundamental change in the conduct of international relations and warfare. In response, a second wave of academics believes that cyber does not represent anything significant since it cannot cause tremendous physical destruction.

The initial decade-long reaction to the advent of the popular use of the internet in the 1990s, and the associated vulnerabilities it presented, was that cyber represented a sea change in the conduct of military affairs. Proponents pointed to the concept of the Revolution in Military Affairs (RMA) and argued that the cyber realm offered a strategic advantage since a fundamental element of the theory of RMA is the collection and control of information. RAND's John Arquilla and David Ronfeldt argued that information is the necessary component to wield power. Particularly, "information… should be treated as a basic, underlying, overarching dynamic of all theory and practice about warfare in the information age."[37] Further, that "cyberwar may raise broad issues of military organization and doctrine, as well as strategy, tactics, and weapons design. It may be applicable in low- and high-intensity conflicts, in conventional and non-conventional environments, and for defensive or offensive purposes." Lastly, they add:

[37] Arquilla, John and David Ronfeldt. "Information, power and grand strategy: in Athena's camp." *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, CA: RAND, 1997. p. 154.

"...we anticipate that cyberwar may be to the 21st century what blitzkrieg was to the 20th century. ... In a deeper sense, cyber war signifies a transformation in the nature of war."[38]

This assessment has continued to thrive among leadership circles in different states. While as Secretary of Defense in 2012, Leon Panetta echoed Winn Schwartau's words from 1991 and warned of a "Cyber Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability... and could shut down the power grid across large parts of the country."[39] The White House's International Strategy for Cyberspace of 2011 codified this sentiment by proclaiming: "When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country," to include a military response.[40] This policy joined the chorus of cyber warnings that likened the threat from cyberspace to that of conventional hostile warfare. This theory of the threat of cyber warfare will be known as the first wave response group.

The retort to the first wave assessment, known as the second wave, argued that since cyber warfare would not likely result in the physical deaths of the enemy or target country, it therefore did not represent a significant change in the conduct of warfare and admonished the first wave academics, policy makers, and commentators as being hysterical and hyperbolic. Without a body count, this second wave assessment refuted

---

[38] Arquilla, John and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, Vol 12, No. 2, Spring 1993, p. 27-32.
[39] Bumiller, Elizabeth and Thomas Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times*, October 11, 2012.
[40] "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." Washington, DC: The White House, May 2011. p. 14.

the claim that cyberwar was a threat equal to conventional hostilities. Rid argues that for a cyber war to occur, there must be lethality, and that a cyberattack has never resulted in death so cyber war has not occurred and will not occur in the future.[41] The second wave contends that cyber war capabilities are akin to any other incremental military technology advancement and do not represent a change in the conduct of warfare. In "The Myth of Cyberwar," Gartzke notes:

> Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable harm on an adversary. In many, perhaps most, circumstances, this will occur only if cyber war is accompanied by terrestrial military force or other actions designed to capitalize on any temporary incapacity achieved via the internet.

Maness and Valeriano argue that there is little evidence that cyber war is or is likely to become a serious threat. They coded dyadic cyber interactions from 2001 to 2011 and using that empirical data, concluded that cyber incidents are a "little-used tactic with low level intensity and few to no long-term effects."[42] Valeriano argues: "The data we have presented here illustrate that cyber disputes are rare. When they do happen, the impact tends to be minimal. Only 20 of 126 possible ongoing rivals engage in cyber combat."[43] However, focusing on the quantity provides a false sense of security and these scholars were using a dataset covering only the first decade of the 2000s. Moore's law[44]

---

[41] Rid, Thomas, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35/1 (Feb. 2012). p. 6–10.
[42] Valeriano, Brandon and Ryan Maness. *Cyber War Versus Cyber Realities*. Oxford: Oxford University Press, 2015. p. 108
[43] Ibid. p. 108
[44] As noted earlier, Moore's law is the observation that the number of transistors in a dense integrated circuit doubles approximately every two years. A modern interpretation is a focus on the increase of cores per die instead of simply clock speed, as was the original Moore's law. A core is a unit that runs in parallel with other cores; a die consists of several cores.

demonstrates that isolating cyber-related research to the first decade of the 2000's ignores 5-6 cyber generations that have occurred in the interim. In addition, Valeriano and Maness' conclusion that cyber does not meet the threat level of a hot war does not preclude its ability to be used successfully in other ways, such as cyber coercion.

The view of the third wave sees a value in the use of the cyber realm for foreign policy, refuting both extremes of the first and second waves and provides several utilitarian options for the use of cyber, one of which is cyber coercion. This third wave has contributed to the literature by providing structured empirical analyses and studying cyber interactions that have actually occurred.[45] Additionally the third wave has improved the dialogue by using middle-range international relations theory[46] and presenting evidence in a policy-relevant, straightforward manner that is neither hyperbolic and based on what-if scenarios nor dismissive since it is unlikely to result in a hot war. The third wave of "middle-range theories attempt to formulate well-specified conditional generalizations of a more limited scope. …[This allows them] to explain different subclasses of a general phenomena."[47]

Scholars following this design in examining the use of cyber for coercive diplomacy include Travis Sharp, Forrest Hare, Daniel Flemming, Neil Rowe and Tim Junio. Sharp argues that cyber has a coercive value through cost imposition and leadership destabilization and uses the 2014 North Korea cyber operation against Sony

---

[45] Sharp, Travis. "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony." *Journal of Strategic Studies*, 2017. Vol 40, Num 7. p. 901

[46] George, Alexander L. and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MIT Press, 2005. p. 266.

[47] Ibid. p. 266.

Pictures Entertainment as a case study to prove his theory. He also spends time refuting the second wave theorists and advances a proxy idea to get at the issue of attribution/credible demand, the Known Coercer Plus Known Demand Standard, which has been borrowed for this research.

In looking at cyber coercion from the victim's side, Forrest Hare employs Buzan's vulnerabilities framework to explain how relative power disparities among states and differing levels of socio-political cohesion within a state can cause them to prioritize and characterize cyber threats differently. He highlights that a concern that stems from these different views on the significance of cyber threats creates a potential for a security dilemma in cyberspace.[48] In a later paper, Hare advances a proposed coercion strategy framework, in the absence of any other working framework in the discipline for this issue, focusing on the deterrence aspect of coercion. He, too, spends ample time refuting the second wave theorists but also argues that "unequivocal attribution is not required"[49] to assess an effective deterrence strategy and provides several examples to demonstrate his argument.

Flemming and Rowe argue that cyber coercion will likely become increasingly prevalent in the future. Further, they argue that cyber coercion can defuse short-of-war conflicts and can offer net cost-benefit, saving potential financial and human costs

---

[48] Hare, Forrest. "The Cyber Threat to National Security: Why Can't We Agree?" *Conference on Cyber Conflict Proceedings, 2010.* Tallinn, CCD COE Publications.
[49] Hare, Forrest. "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." *Fourth International Conference on Cyber Conflict,* 2012. Tallinn, CCD COE Publications.

associated with warfare.[50]

In challenging second wave scholars such as Rid and Liff, Junio believes that cyber war, defined as "a coercive act involving a network computer attack"[51] is possible and he seeks to correct "the [second wave] narrative that cyberwar is improbable."[52] Junio provides an overview of a structured scientific inquiry testing the effect of information technology (IT) on the assumptions contained in Fearon's "Rational Explanations for War" describing the conditions in which war should not occur. Junio concludes that the effect of IT on each assumption makes it either less tenable or the same as other kinds of warfare. In addressing the second wave, Junio offers that "if the perception that cyber weapons are non-lethal comes to be widely-perceived (as Rid would prefer), it is reasonable to conclude that the threshold for their use will be lower than other kinds of weapons - even if the cost of cyberattacks is greater."[53] He demonstrates not only the destructive potential of cyber war but illustrates how cyber statecraft increases the potential for conflict.

This research contributes to the third wave in a number of ways including by presenting policy-relevant recommendations as well as demonstrating that the conventional wisdom on two widely-cited case studies should be significantly modified. This reversal is shown by introducing a Utilitarian approach and examining the case

---

[50] Flemming, Daniel and Neil Rowe. " Cyber Coercion: Cyber Operations Short of Cyberwar." This paper appeared in the proceedings of the 10th International Conference on Cyber Warfare and Security, Skukuza, South Africa, March 2015.
[51] Junio, Timothy. "How Probably is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate." *The Journal of Strategic Studies*, Vol 36, Num 1, 2013. p .126.
[52] Ibid. p .132.
[53] Ibid. p .130.

studies over a longer temporal period, thus revealing additional data points that require a reevaluation of the common interpretation of these cases. Further, this research extends the variables that favor coercive diplomacy within cyber statecraft and shows how the presence or absence of these variables can result in divergent outcomes. This set of expanded variables include 1) financial costs for the victim, 2) audience costs for the victim, 3) leadership destabilization potential through targeting of leadership, and 4) the amount of pressure on leadership. Finally, this research fuses social science approaches to cyber attribution with the commercial cybersecurity industry access and techniques to attain attribution, overcoming the attribution obstacle noted in the earlier literature.

CHAPTER 2: CYBER COERCION

You can engage in a shift in relative power without going to war, …you may look for a new scene in which to exploit capabilities in such a way that you might be able to achieve strategic intent. If you understand that pivot, this notion of campaigns with strategic intent, leveraging cyber, cyber campaigns I should say, then the need to engage on a continuous basis, primarily from a defensive motivation, and build more resiliency, …in fact requires you, given the nature of the technology and given the nature of the space, to be outside your network. If you are defending on your network… you're chasing.[54]

Are cyber capabilities useful to elicit certain responses from a victim? Applying George's seven conditions that favor coercive diplomacy is a good start in examining this question. However, George's approach for traditional coercive diplomacy is not sufficient to explain the divergent outcomes seen across cases of cyber coercion. Instead, it is the interaction among George's seven conditions, along with additional independent variables, combined with changing temporal values that contribute to determining a victim's response to cyber coercion against soft, countervalue targets. It is this extension of George's original conditions that can explain why cyber coercion produces certain responses in some circumstances and different responses in others. Traditional studies do not do this – *previous scholarship has been too binary and focused narrowly on success/failure, but also too restricted temporally***.** This chapter will also provide the applicable international relations theoretical literature to include George's theory of coercive diplomacy and forceful persuasion, and, offense-defense theory, as posited by

[54] Richard Harknett, Professor and head of the Department of Political Science, University of Cincinnati; presenting at the Cato Institute "Cyber Warfare, Coercion, and Restraint," May 9, 2019.

scholars Robert Jervis, George Quester and Stephen Van Evera and its application to the cyber realm.[55]

[55] Jervis, Robert. "Cooperation under the Security Dilemma." World Politics, 1978, vol. 30, no. 2. p. 167 214; Quester, George. "Offense and Defense in the International System." In Michael Brown, Owen Cote Jr., Sean Lynn-Jones, and Steven Miller (eds.) Offense, Defense and War. Cambridge: MIT press, 2004. p. 51-68; and Van Evera, Stephen. "Offense, Defense and the Causes of War." International Security, Spring 1998, Vol. 22, No. 4. See also Glaser, Charles L. & Chaim Kaufmann: "What Is the Offense-Defense Balance and How Can We Measure It?", International Security, Spring 1998, Vol. 22, No. 4. p. 44-82.

Why is Cyber Unique?

Cyber capabilities are distinct from conventional weaponry in nature, behavior, cost, and power calculation. However, early academic scholarship sought to compare a state's options for using cyber capabilities with the Cold War-era nuclear proliferation literature and this narrative had significant stickiness for the study of strategy in cyberspace. Much of the 1990's and early aughts literature finds scholars borrowing theories and strategies from the nuclear proliferation literature[56] to apply to the cyber realm; "…indeed much of the lexicon of cyber strategy is drawn from the Cold War."[57] While we can use some of these theories to explain relations among states during times of low-level disagreement and conflict, and apply them to cyber, we must distinguish cyber capabilities from other types of pressure campaigns used for coercion among states. Schelling's work in nuclear deterrence is often applied to the cyber realm and his seminal work on strategy and bargaining in the nuclear age, *Arms and Influence*, provides a foundation that we can employ to assess to usefulness of cyber in coercive diplomacy.

Cyber statecraft offers a number of benefits for conflict resolution for both the aggressor and the victim, depending on the choices each player makes. For the victim, there is the range of reactions from doing nothing or ignoring the demands, to

---

[56] A number of scholars have demonstrated the progression of the study of political implications for cybersecurity from relying heavily on the nuclear proliferation literature in the 1990s and 2000s to forming its own area of study in the 2010s onward. This history is captured well in: Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Washington DC: Cyber Conflict Studies Association, 2013. See also, Fred Kaplan, *Dark Territory: The Secret History of Cyber War.* New York: Simon and Schuster, 2017.

[57] Lewis, James. "Toward a More Coercive Cyber Strategy." *Center for Strategic and International Studies,* March 4, 2021. p. 2.

acquiescing, defending, counter-attacking or some combination of these responses. As one scholar noted:

> "The uncertainty of cyberspace, instead of creating spiral dynamics and security dilemmas, allows people the space to slow down. It creates anxiety, if you are a state that does not want to respond anyway, it gives you the uncertainty to be able to back out. Oh, I could not get attribution! Oh, I am not sure if that [the cyber action] is really a cyber thing? …And if your tendency is not to retaliate then cyberspace actually gives you the ability to not retaliate. To have this nice space that is created in which you can have some level of confrontation… but what we need to think about in our strategies is about articulating much more clearly what that confrontation looks like."[58]

Depending on the nature of the attack, if it is one where a victim does not incur audience costs nor financial costs, a victim may choose to acquiesce quietly to stave off future embarrassment and save face. However, if the aggressor chose to publicly announce the cyberattack or publicly embarrass the victim, thus driving up victim audience costs and potentially financial costs, then a victim may choose a different response in order to preserve their status, protect their dignity, and/or deter other states and non-state actors from also attacking.

Nature and Behavior

The strategy considerations for cyber statecraft should not be shoved under the umbrella of extended nuclear deterrence theory when looking for explanatory theories or designing options for statecraft. Cyber capabilities and weapons are inherently secretive

[58] Jacquelyn Schneider, Assistant professor in the Strategic and Operational Research Department, U.S. Naval War College; presenting at the Cato Institute "Cyber Warfare, Coercion, and Restraint," May 9, 2019.

in nature and can suffer a short shelf life. States may not risk a cyber conflict quickly;[59] since, unlike conventional weapons, some cyber capabilities can be one-and-done options once the vulnerability is revealed to an adversary, or they may be reusable techniques.

The National Academy of Sciences noted that cyber capabilities have three characteristics that differentiate them from kinetic weaponry. Namely, cyber capabilities are:

> "easy to use with high degrees of anonymity and with plausible deniability, making them well suited for covert operations and for instigating conflict between other parties; are more uncertain in the outcomes they produce, making it difficult to estimate deliberate and collateral damage; and involve a much larger range of options and possible outcomes; and, may operate on time scales ranging from tenths of a second to years, and at spatial scales anywhere from "concentrated in a facility next door" to globally dispersed."[60]

Cost

The cost of conducting cyber operations can be incredibly cheap or extremely investment-heavy, depending on the type of operation, the sophistication of the target, and the expected duration. In the case of a sophisticated hard target, one does not just replicate more code and lob them at the adversary; "…the cost of a cyber weapon, which is almost entirely in R&D [research and development], cannot be amortized over as many

[59] Axelrod and Iliev analyze the optimal timing for the use of cyber capabilities and offer a mathematical model to determine the best timing to use a particular capability, especially given that its first use may prevent it from being used again in the future. The full citation is: Robert Axelrod and Rumen Iliev. "The Timing of Cyber Conflict." *Proceedings of the National Academy of Sciences of the United States of America.* January 28, 2014. p. 1298-1303.
[60] Owens, William A, Kenneth W. Dam and Herbert S. Lin (eds.), "Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities". *National Research Council*, 2009; p. 24.

targets as would be the case for a kinetic weapon. This fact necessarily increases the cost-per-target destroyed."[61] A missile can be used as a deterrent for years; conversely, cyber capabilities are one patch away from being rubbish.

That being said, some cyber capabilities do not require significant research and development funding, some can be easily purchased or created with minimal investment, which is part of why they are an attractive option for small or weak states, and non-state actors, to exert influence or power. Writing in 2011, Joseph Nye observed: "90 percent of military telephone and Internet communications travel over civilian networks. Finally, because of the commercial predominance and low costs, the barriers to entry to cyber are much lower for non-state actors."[62] The barriers to entry for non-state actors may be low, but it also means that those capabilities are likely be used against soft targets or unsophisticated adversaries.

Power Calculation

While a state may have a reputation for its offensive cyber aptitude, unlike conventional arms, offensive and defensive cyber capabilities are a constantly changing game and it is difficult to measure one's relative cyber power against an adversary, especially one prone to bombastic speech who may overstate their abilities. A state's offensive cyber capabilities are kept secret, so when a state or non-state actor is deciding

[61] Lin, Herbert. "Oft-Neglect Cost Drivers of Cyber Weapons," Council on Foreign Relations Net Politics (online blog), December 14, 2016, http://blogs.cfr.org/cyber/2016/12/14/oftneglected-cost-drivers-of-cyber-weapons/.
[62] Nye Jr., Joseph. ""Nuclear Lessons for Cybersecurity?" *Strategic Studies Quarterly*, Winter 2011. p. 22.

whether to use their cyber capabilities offensively against an adversary for coercive purposes, it is tricky to calculate one's chances for success at the outset since the adversary may have an extremely competent defense or may withhold its relative cyber power capabilities during increased tension or a cyber-based coercive conflict to preserve for future use. That is, "the malleability of cyberspace offers, in the words of Bruce Schneier, a unique 'window of exposure' for cyberattacks to be effective."[63] As Richard Harknett noted at a CATO Institute policy forum in 2019:

> You can engage in a shift in relative power without going to war, …you may look for a new scene in which to exploit capabilities in such a way that you might be able to achieve strategic intent. If you understand that pivot, this notion of campaigns with strategic intent, leveraging …cyber campaigns, then the need to engage on a continuous basis, primarily from a defensive motivation, and build more resiliency, …in fact requires you, given the nature of the technology and given the nature of the space, to be outside your network. If you are defending on your network… you are chasing.[64]

Unlike conventional arms capabilities which can be debuted at parades as they roll down the promenade, counted and assessed for range and lethality by adversary states,[65] for cyber capabilities one cannot see the capabilities consisting of ones and zeros

---

[63] Referenced in Smeets, Max. "A matter of time: On the transitory nature of cyberweapons." *Journal of Strategic Studies*, 2018: 41:1-2, 6-32. p. 13. Original quote from Bruce Schneier, 'Crypto-Gram', September 15, 2000. Located at: https://www.schneier.com/crypto-gram/archives/2000/0915.html

[64] Richard Harknett, Professor and head of the Department of Political Science, University of Cincinnati; presenting at the Cato Institute "Cyber Warfare, Coercion, and Restraint," May 9, 2019.

[65] "North Korea Stages Show of Force with New Missiles During Parade," *Reuters*, September 9, 2018. https://www.reuters.com/article/us-northkorea-missiles-parade/north-korea-stages-show-of-force-with-new-missiles-during-parade-idUSKBN1FT0U8 Accessed September 20, 2019. Additionally, multiple defense reporters and defense researchers from RAND and elsewhere were live tweeting this parade, their observations about new weaponry and potential lethality estimations as well as observations about weaponry that is known to exist in North Korea but

that an adversary may harbor at any given time. These cloaked capabilities have consequences for relative power calculations within the larger coercion calculus.

Of those who believe the cyber threat is exaggerated, the focus is myopic; concentrating on body counts when the discipline needs to approach this as a tool applicable across a spectrum of options. The "cyber threat" does not stem from the malicious code, but from the human intent to use it against a specific target.[66] When talking about the employment and risk assessment of cyber, scholars and policymakers often speak in terms of effects, residual body counts and the extreme of possible destruction. We discuss the ethics of using this suite of cyber-based weapons and capabilities with respect to the furthest extent of damage possible: will it result in the loss of human life? This is a short-sighted approach.

Looking at the cyber arena through the lens of coercion (comprised of deterrence and compellence) begs the question: how can cyber actions, below the level of armed conflict, be effectively used during peacetime to change a victim's behavior and elicit a desired response? Instead of simply trying to destroy an adversary's systems, can one use it just enough to exact costs that provoke a response that is advantageous to an aggressor's desire? When assessing cyber options, cyber conflict, cyber war, or actors in the cyber realm, the academic analysis is often focused on military planning, military

---

were not on display. This analogy is used to illustrate the difficulty in judging an adversary's cyber capabilities since there is no equivalent to a military parade in the cyber realm.

[66] Libnicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007. Also, Koh, Harold Hongju. "The Emerging Law of the 21st Century War." *The Brookings Institute*. Breyer Lecture presentation, April 1, 2016.

tactics, lethality, and the benefits to the military, not to diplomacy.[67] However, the concept of using cyber for coercive diplomacy, as we will see in the case studies, can be effective for goals beyond simply military dominance, like eliciting a change in behavior, if executed correctly.

[67] Flemming, Daniel and Neil Rowe. "Cyber Coercion: Cyber Operations Short of Cyberwar." ICCWS 2015 - The Proceedings of the 10th International Conference on Cyberwarfare and Security. Edited by Jannie Zaaiman and Louise Leenan. 2015. p. 95

Attribution – Is It Still a Problem? Strategies for Achieving Attribution

One criticism of the use of cyber capabilities for successful coercive diplomacy is the issue of attributing the attack and understanding the demand. George notes that the "clarity of objectives and demands" and knowing the adversary are relevant variables for a successful use of coercive diplomacy.[68] It is often difficult in the cyber realm to immediately attribute an attack with absolute certainty, but that assumes absolute certainty is required. Given ongoing tensions, victims can often make a confident assessment supported by technical cyber forensics within hours or days of an attack. Added to that, Healey provides a Spectrum of State Responsibility that can be used to assess attribution in more granularity and will be discussed in detail below. Taken together, the technical information combined with Healey's Spectrum, show how the problem of attribution, a problem that is oft-used as an excuse for why cyber coercion is impossible, can be surmounted. This research argues that given the less-than-lethal threat, where there is a decent confidence of the coercer's identity and the coercer's demand a victim can use the technical data to assist in determining a ranking on Healey's spectrum, react accordingly and that "unequivocal attribution is not required."[69] Cautioning, Rid and Buchanan offer a systematic model, the Q model, for attributing intrusive cyber operations and note that it is a layered, complex art that requires skill to

---

[68] George, Alexander. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. Washington, DC: United States Institute of Peace Press, 1991. p. 76-81. See also Alexander L. George and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994. p. 280-281.

[69] Hare, Forrest. "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." 2012 4th International Conference on Cyber Conflict, 2012. NATO CCD COE Publications.

be successful.[70] While Rid and Buchanan's Q model presents a useful strategy for how to tackle the problem of attribution, this dissertation offers a different approach that is an amalgamation of Sharp's approach and Healey's Spectrum combined with cybersecurity research and cyber assessments based on the specific code involved in a cyberattack.

Substantial previous scholarship frames the value of cyber coercion as one that is significantly hindered by problems of attribution; that the ambiguity of attribution in cyberspace undermined the credibility of the threat and thus the potential for cyber coercion in general.[71] The issue of attribution has been treated in the literature like an unbeatable bogeyman that prevents serious scholarship from assessing the usefulness of cyber coercion; it is not.[72]

As Hare notes, "many have focused on the challenges of achieving conclusive attribution of malicious actors."[73] For some scholars, the issue of attribution is of paramount importance, often citing that the attacker must be explicitly known in order to cause the effect sought and without proper attribution the rest of the coercion calculation is meaningless. However, this is a flawed interpretation; one that does not properly incorporate the abilities of the commercial cybersecurity industry to provide reasonable

---

[70] Rid, Thomas and Ben Buchanan. "Attributing Cyber Attacks." *The Journal of Strategic Studies.* Vol 38, Num 1-2. p. 30.

[71] Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND, 2009; National Research Council, ed., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010).

[72] Many of the same problems afflict the study of certain national security issues but this has not prevented the emergence of thriving academic literature on these topics.

[73] Hare, Forrest. "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." *4th International Conference on Cyber Conflict*. NATO CCD COE Publication, Talinn, Estonia, 2012. p. 126

attribution, as well as reasonable situational attribution using Sharp's and Healey's strategies described below, and therefore remove "attribution" as an obstacle to determining the value of cyber coercion. For states that may not be able to conduct attribution based on government capabilities, they are able to purchase these services from a variety of global cybersecurity companies who are extremely adept in reasonably determining the actor, as will be described further below. A simplified taxonomy of attribution is the following:

1. Government-operated: planned, funded and run by government/military officials using government/military infrastructure
2. Government-associated: planned, funded and run by contractors associated with the government, and with tacit approval of the government
3. Government-sponsored: government funded, run by non-government organizations responsible for the planning and operations
4. Government-allowed: criminals and independent hackers who conduct activities on their own, sometimes with the encouragement of the government but not necessary, and the government allows them to conduct operations as long as they do not attack things the government does not want attacked

As Rid and Buchanan remind us, attribution is "an exercise in minimizing uncertainty on three levels: tactically, attribution is an art as well as a science; operationally, attribution is a nuanced process not a black and-white problem; and

strategically, attribution is a function of what is at stake politically."[74] Jason Healey provided a more in-depth spectrum of state responsibility that can aid in determining attribution. It helps to delineate whether a national "ignores, abets, or conducts and attack… [and] the spectrum starts from a very passive responsibility … up to a very active responsibility."[75] Healey's Spectrum of State Responsibility is as follows:[76]

1. State-Prohibited – the government will help stop third party attacks
2. State-Prohibited but Inadequate – The government is cooperative but unable to stop third party attacks
3. State-Ignored – the government knows about third party attacks but is unwilling to take any official action
4. State-Encouraged – Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5. State-Shaped – Third parties control and conduct the attack but the state provides some support
6. State-Coordinated – The government coordinates third party attackers such as by "suggesting" operational details
7. State-Ordered – the government directs third party proxies to conduct the attack on its behalf
8. State-Rogue-Conducted – out-of-control elements of cyber forces of the government conduct the attack
9. State-Executed – the government conducts the attack using cyber forces under its direct control
10. State-Integrated – the government attacks using integrated third-party proxies and government cyber forces

Finally, scholar Travis Sharp offers a solution to this issue of exact attribution that often plagues analysis of cyber threats, by providing a working description of this spectrum of certainty that he calls the Known Coercer plus Known Demand Standard for

---

[74] Rid, Thomas and Ben Buchanan. "Attributing Cyber Attacks." *The Journal of Strategic Studies*, 2015 Vol. 38, Nos. 1–2, p. 4.
[75] Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." *The Atlantic Council*, January 2012.
[76] Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." *The Atlantic Council*, January 2012. p. 2-3.

Classifying Cyber Coercion Attempts. Employing this spectrum of certainty, combined with Healey's Spectrum of State Responsibility, and viewing it through the general taxonomy of attribution allows us to surmount the strict attribution problem while accounting for attribution using a given range. Sharp's approach is shown in Figure 2:[77]

Figure 2.

Known Coercer + Known Demand

Victim Certainty about Coercer's identity	More Certain	Less Certain
More Certain	Cyber operation **does** qualify as cyber coercion attempt North Korea vs. Sony, 2014	Indeterminate classification Attack on DNC, 2016
Less Certain	Indeterminate classification Attack on Estonia, 2007	Cyber operation **does not** qualify as cyber coercion attempt

Victim's Certainty about Coercer's Demand

In additional to the qualitative approach to help determine attribution, we can rely on commercial cybersecurity companies to illuminate provenance of an attacker through technical data. Determining attribution is a non-trivial issue for some second-wave scholars, so borrowing cybersecurity best practices to assess attribution overcomes this

[77] Sharp, Travis. "Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony." *Journal of Strategic* Studies, 40:7, April 2017, p. 898-926.

issue. There are two kinds of attribution in cybersecurity terms: intrusion cluster attribution and the definitive "county X did this attack" attribution.

Intrusion cluster attribution can usually be performed in a matter of hours with reasonable certainty of the actor. These are generally categorized as either an UNC, an uncategorized intrusion cluster, or an APT, an Advanced Persistent Threat. Some UNCs are eventually categorized as an APT, and some maintain UNC status.[78] An APT is defined as "groups that receive direction and support from an established nation state."[79]

One prime example of this is the Russian intrusion set known as the "Dukes."[80] This intrusion set has been around for over a decade and each iteration shares characteristics with previous generations. These characteristics include: the same IP hosting the malware; Russian wording found in the code; Russian time zones used in the compiling; hardcoded IPs; specific command and control code; reused domain names; similarities in the writing style of the code; similarities in how the code is organized; similarities in sections of the code showing up in the exact same order.[81] Cybersecurity

---

[78] Berninger, Matt. "Going ATOMIC: Clustering and Associating Attacker Activity at Scale." *FireEye*, March 12, 2019. Located at: https://www.fireeye.com/blog/threat-research/2019/03/clustering-and-associating-attacker-activity-at-scale.html and accessed on January 15, 2021. See also: Vanderlee, Kelli. "DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors." *FireEye*, December 17, 2020. Located at: https://www.fireeye.com/blog/products-and-services/2020/12/how-mandiant-tracks-uncategorized-threat-actors.html and accessed on January 15, 2021.

[79] "Advanced Persistent Threat Groups." *FireEye*. Located at: https://www.fireeye.com/current-threats/apt-groups.html and accessed on January 15, 2021. See also, Pieter Arntz, "Explained: Advanced Persistent Threat" *MalwareBytes Labs*, July 26, 2016. Located at: https://blog.malwarebytes.com/101/2016/07/explained-advanced-persistent-threat-apt/ and accessed on January 15, 2021.

[80] F-Secure White Paper. "The Dukes 7 Years of Russian Cyber Espionage," September 2015. Data from related Dukes intrusion sets continue to be seen in hacks today.

[81] Ibid.

companies can take a piece of malware and perform a commonality look across all the other malware samples (of the same file type) within their own corporate storage (20+ billion examples) and against collections like Virus Total (~4 billion examples), to determine intrusion set attribution within a matter of hours and get a high confidence result. What was a very difficult undertaking a decade ago, is now a nearly automated process based on a rich history of malware used across the world that private industry has catalogued.[82]

In the case of the first "Duke" referenced above, PinchDuke was used against Chechen targets in November 2008.[83] The Russians hardcoded the targets. Since then there have been ten related intrusion sets created that have been used in over twenty hacking campaigns spanning over 12 years, and each have been identified by the cybersecurity industry.[84]

The commercial cybersecurity industry may be able to attribute down to a detailed level of which actor within a country is responsible for a particular type of malware based on the characteristics described above. If the commercial cybersecurity industry is unable to attribute down to the level of a specific actor within a country and knowing the country of origin is not a detailed enough attribution for the cyber coercion calculation, then we can employ Healey's Spectrum of State Responsibility to get a better level of attribution within a state.

---

[82] Ibid.
[83] Ibid. p. 4.
[84] F-Secure White Paper. "The Dukes 7 Years of Russian Cyber Espionage," September 2015.

As an example of the level of detail that the commercial cybersecurity industry can attribute, the F-Secure White Paper describes that in the initial 2008 PinchDuke malware, the software engineers used a particular command and control server. For the 2010-2015 CosmicDuke malware they re-used this command and control server[85] and borrowed techniques and components from PinchDuke. This was a clear indication that these two intrusion sets shared command and control features and therefore were run by the same outfit. [86]

Another example comes from Crowdstrike's assessment in 2015 that it "observed multiple malware samples with suspected association to DPRK actors throughout 2015. …Many of the samples were linked back to campaigns beginning in 2014, suggesting either a continuation of previous activity, or a resurgence of those programs."[87] With over a decade of internet cyber aggression history, attribution in 2021 is no longer the insurmountable, mammoth challenge that it was in 2005 and should not be seen as a absolute barrier to identifying cyber coercion actors.

[85] Ibid. p. 7.
[86] Ibid. p. 7-11, 25.
[87] Crowdstrike Intelligence Report. "2015 Global Threat Report." *Crowdstrike*, 2015. p. 31

Key Concepts and Definitions

Applying George to cyber: What is coercion in the cyber realm?

States employ diplomacy and the use of force to achieve political objectives. The options for a state to threaten the use of force has expanded with the advent of the cyber domain. This study assesses the use of the cyber domain as a means of coercion to influence behavior, both between states and between states and non-state actors. In order to understand the study, one must have a clear understanding of coercion theory and how it applies to cyber statecraft.

Coercion is the power to hurt[88] and coercive diplomacy consists of knowing the fears and vulnerabilities of your adversary and effectively exploiting them. Coercive diplomacy is conveying a sense of coercive reality to attempt to reverse actions already undertaken, deter future activities, or influence a future decision by an adversary through the use of threats and limited force to persuade. The proximate purpose of coercive diplomacy is to create fear and to communicate a fearsome reality if the adversary continues with its original plan. Broadly defined, it is the use of threats to influence another's behavior and encompasses both compellence, as coercion to act, and deterrence, or coercion not to act.[89] "Writing on coercion requires modesty... the topic

[88] Schelling, Thomas C. *The Strategy of Conflict*. 2nd ed., Harvard University Press, 1990. See also Byman and Waxman (2002) and Robert Pape's *Bombing to Win: Air Power and Coercion in War*. Cornell University Press, 1996.

[89] This is a broad reference to Schelling, Thomas. *Arms and Influence.* New Haven: Yale University Press, 1966. p. 2–6; and Daniel Byman and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might.* New York: Cambridge Univ. Press, 2002. p. 1 and Joseph Nye Jr., ""Nuclear Lessons for Cybersecurity?" *Strategic Studies Quarterly*, Winter 2011.

itself defies easy description."[90] Scholars such as Schelling and modern theorists like George, Byman and Waxman provide detailed interpretations of their definition and use of coercion theory.

Schelling's definition of coercion includes both compellence and deterrence. He notes, "the threat that compels rather than deters often requires that the punishment be administered *until* the other acts, rather than *if* he acts.[91] Schelling remarks:

> To inflict suffering gains nothing and saves nothing directly; it can only make people behave to avoid it. The only purpose, unless sport or revenge, must be to influence somebody's behavior, to coerce his decision or choice. To be coercive, violence has to be anticipated. And it has to be avoidable by accommodation. The power to hurt is bargaining power. To exploit it is diplomacy - vicious diplomacy, but diplomacy.[92]

For Schelling, it is the threat of this violence and/or damage, followed by more damage, that can make someone comply with one's demands or discontinue an unwanted behavior. He asserted that coercion is the exploiting of the calculus of the costs and benefits of action, short of brute force, and operated by raising the costs or risks beyond a tolerable level.[93]

The adversary makes this decision based on their own cost-benefit calculation. At a high level, if the consequences of the threat of violence or destruction is less than the demand, according to the target of the threat, then it is unlikely the target will capitulate.

---

[90] Byman, D and M Waxman. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might.* UK: Cambridge University Press, RAND, 2002. p. 23.
[91] Schelling, 1966.
[92] Schelling, Thomas. "The Diplomacy of Violence." *Essential Readings in World Politics*, Karen Mingst and Jack Snyder, eds. New York: WW Norton & Company, 2004. p. 301
[93] Schelling 1966.

If the threat of violence or destruction is greater than the perceived threshold the target of the threat is willing to endure, then they are more likely to yield. In short, "Coercion requires finding a bargain, arranging for him to be better off doing what we want — worse off not doing what we want — when he takes the threatened penalty into account."[94] The literature on coercion suggests various conditions that need to be met in order for success.

Alexander George provided a comprehensive list of seven conditions for successful coercion: clarity of the objective, strength of motivation, asymmetry of motivation, sense of urgency, adequate domestic and international support, opponent's fear of unacceptable escalation, and clarity concerning the precise terms of settlement of the crisis.[95] George notes that no single condition can explain successful coercion but improving the status within each condition contributes to overall success. For George, successful coercion depends on the specific factors at play in a particular situation, those factors determine the strategy, and maximizing these seven conditions should result in successful coercion. Each of these seven conditions can be applied to the theory of cyber coercion as shown below, but do not fully explain the outcomes in the cases studied.

---

[94] Schelling, Thomas. "The Diplomacy of Violence." *Essential Readings in World Politics*, Karen Mingst and Jack Snyder, eds. New York: WW Norton & Company, 2004. p. 302

[95] George, Alexander. *Forceful Persuasion.* Washington, DC, United States Institute of Peace Publisher, 1991. p. 76-81.

Clarity of the objective

For George, clarity of the objective is not always essential, but the lack of clear objectives can be an obstacle to successful coercive diplomacy.[96] A clear understanding of the objective by all involved and a defined demand ensures that the adversary will not misperceive what is at stake and will respond accordingly. For the cyber realm, due to the secret nature of operating in cyberspace, a lack of clarity of the objective can make bargaining and coercion more complicated, even when that objective has been communicated elsewhere. It can be difficult to definitively marry the actions taken in the cyber realm to the overt threats or demands made in another domain like the media or in diplomatic channels.

Strength of Motivation

The coercer must be motivated to initiate the crisis and maintain that motivation throughout the crisis.[97] The adversary should perceive a significant strength of motivation on the part of the aggressor for the coercion to credible and convincing. For strength of motivation in cyber, the coercer must not only be motivated to enter a crisis but willing to leverage cyber capabilities, some of which may be single-use, and therefore requires significant motivation to enter a crisis. A single-use cyber tool may also serve to signal that the aggressors have an extremely high level of motivation since they are willing to leverage that single-use tool for a particular situation and the victim should act

[96] George, Alexander. *Forceful Persuasion.* Washington, DC, United States Institute of Peace Publisher, 1991. p. 76.
[97] Ibid. p. 76-77.

accordingly.

Asymmetry of Motivation

The complement to George's strength of motivation is asymmetry of motivation. "Coercive diplomacy is more likely to be successful if the side employing it is more highly motivated by what is at stake in the crisis than its opponent."[98] One critical aspect of successful coercion is that if an adversary believes the coercer is more highly motivated to achieve their goals than the victim is to prevent them, then the coercion will be successful.[99] For cyber, this can be more complicated, again given the secretive nature of cyber interactions. A victim may underestimate their motivation in a particular crisis until the coercer engages in cyber conflict, ranging from cyber disruption to cyber degradation, thus driving up the costs for the victim and changing the motivation calculus vis-a-vis the adversary.

Sense of Urgency

The coercing power must convey a credible sense of urgency and, more importantly, the adversary must accurately perceive this sense of urgency.[100] As George reminds us, the credible sense of urgency can encourage an adversary to comply and can lead to successful coercion. However, a sense of urgency can also work against the

---

[98] George, Alexander. *Forceful Persuasion.* Washington, DC, United States Institute of Peace Publisher, 1991. p. 77.
[99] Ibid. p. 77.
[100] Ibid. p. 78.

aggressor when the adversary feels pressured to respond quickly and therefore prefers to go to war as opposed to capitulating to urgent burdensome demands.[101]

For cyber, a sense of urgency can be credibly communicated or proven with low level cyber actions that ratchet up the pressure on an adversary. A higher sense of urgency is often only felt after an aggressor has taken an action in the cyber realm and the adversary is suffering the consequences, but that might also have the backlash effect described above; a credible sense of urgency is a delicate balance to communicate from aggressor to adversary.

Adequate Domestic and International Support

"A certain level of political support at home is needed for any serious use of coercive diplomacy."[102] The degree of domestic support may be partially dependent upon how long a crisis lasts, but overall, the domestic and international backing, or lack thereof, is a contributing factor the success or failure of coercive diplomacy.[103]

For cyber, if a coercive action gains broad domestic and/or international support, and the coercive threat is seen as something necessary and proportional, it ratchets up the pressure for the adversary to capitulate. As credible voices in the domestic and/or international arenas express support for a coercive action, the adversary may face domestic audience costs that force them to capitulate. However, this can also backfire, and an adversary's domestic support may increase if the polity feels bullied or cornered

[101] Ibid. p. 78.
[102] Ibid. p. 78.
[103] Ibid. p. 79.

by the international community, therefore decreasing the likelihood of successful coercive diplomacy.

As with most tools of diplomacy, for cyber coercion there is a fine line between success and failure and building the right coalition that heightens pressure while also allowing the adversary to save face when agreeing to the demands is tricky. As Robert Art argues, coercive compellence can be more difficult than deterrence because "it demands more humiliation from the compelled state."[104] Actions like blacking out online abilities (e.g. banking and financial sectors), disrupting cyber-dependent utility infrastructure, or publicly belittling a population or leader, can coalesce disparate public opinion in support of the coerce. If this happens, the coercer can decrease the likelihood of successful coercive diplomacy while simultaneously accidentally helping build support for their adversary's position.

Opponent's Fear of Unacceptable Escalation

To have successful coercion, a coercer needs to motivate an adversary to surrender to one's demands, and a key factor is heightening pressure and signaling to the adversary that the coercer is willing to exceed the adversary's acceptable aggression threshold. The coercer promises that the adversary will feel more pain, that the coercer is willing to escalate to a higher level of pain, and that level is unacceptable to the adversary, so the adversary ought to surrender to the coercer's demands. For this to work

[104] Art, Robert J. "To What Ends Military Power." *International Security* 4, no. 4 (Spring 1980): 10.

successfully, there is a timing component, and it is beneficial if the coercer signals willingness to escalate in the initial or early interaction, so it is clear to adversary as they make their own strategic calculations.[105]

When applied to cyber, the opponents fear of unacceptable escalation can quickly be met if the target in question is one of national critical function such as electrical infrastructure, water supply, transportation systems or financial services. These are the most important functions in modern societies and threatening to disrupt them via cyber means may contribute to the success of a cyber coercion operation. However, as demonstrated in the case study on Estonia, going beyond the threat and actually paralyzing some of these national critical functions can backfire on the coercer, prompting the leadership and/or population to consolidate and unify against the coercer as a common enemy.

Clarity Concerning Precise Terms of the Settlement of a Crisis

As George notes, not only is the clarity of the objective necessary, but there must also be clarity of the coercer's terms for resolution. "It may be necessary in some cases… for the coercing power to formulate rather specific terms regarding the termination of the crisis the two sides have agreed upon and to establish procedures for carrying out these terms and verifying their implementation."[106]

---

[105] George, Alexander. *Forceful Persuasion.* Washington, DC, United States Institute of Peace Publisher, 1991. p. 79-80.
[106] George, Alexander. *Forceful Persuasion.* Washington, DC, United States Institute of Peace Publisher, 1991. p. 80.

For the coercing power in cyber, a lack of clarity in the terms of the settlement can contribute to complicating an already obtuse exchange. As noted above, due to the secretive nature of the cyber realm, it can be challenging to link overt demands to cyber actions and that challenge can also extend to the adversary's understanding of what sort of palpable solution might be acceptable to a coercer. Therefore, it is of utmost importance that both coercer and victim are clear on how a coercive cyber interaction can end, and what each side wants and is willing to give to end a conflict before it escalates.

For the victim in cyber coercion the terms of settlement are important and can take several forms to include: a return to the previous operational state, if possible; a commitment from the coercer to remove itself from the victim's networks; a request to return and/or delete files or data; or a request for an accounting of the cyber actions taken. As the victim in this interaction, however, they are the recipient of the threat and cyberattack and therefore likely do not have the power position in the negotiation to demand any terms of settlement. However, it is important to note the range of what a victim's requests could include in cyber coercion terms of settlement.

Deterrence and Compellence in Cyberspace: Counterforce, Countervalue, and Cyber Coercion

A main component in coercion is target choice and different target types will result in different levels of audience costs and financial costs. In conventional warfare, targets are divided into two categories: countervalue targets and counterforce targets. As noted earlier, countervalue targets are those that do not pose an overt military threat and are most often defined as civilian population centers such as towns and cities, but also include non-military government targets. Conversely, counterforce targets are those that pose a military threat, and consist mostly of government and military personnel and military controlled geographic targets. We can apply this target distinction to cyberspace and this research is scoped to look at soft, countervalue target choices.

In the case of North Korea versus Sony, successful cyber coercion resulted in imposing costs and destabilizing leadership through countervalue targeting since the target was a purely civilian commercial entity. In the case of Russia versus Estonia, Russia targeted countervalue targets including non-military government targets, a blend that eventually backfired in some respects but also provided a value to Russia.

Tolerance for the victim audience costs of countervalue targets is often much lower than it would be for victim counterforce targets; plainly, states see daily efforts to hack, scan or intrude into military and government networks and systems[107] and therefore

[107] Lindsay, Jon and Erik Gartzke. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." In Kelly M. Greenhill and Peter J. P. Krause, eds., *The Power to Hurt: Coercion in Theory and in Practice.* New York: Oxford University Press, 2018. p. 181

there is a level of tolerance for that daily activity. Major hacking events against significant civilian targets occur less often, and when they do, they typically suffer larger audience costs for the victim. For cyber coercion, as costs grow it is often less painful for a victim to comply with the demand than to continue to suffer increasing audience costs.

There is also a significant difference in audience costs between immobilizing a military vehicle located on a military base and disabling a CEO's pacemaker to cause a fatal result. In the first case, it is a military counterforce target which is typically seen as government-backed and resourced and, in this example, safe because they are located on a base so therefore it would not necessarily have significant audience costs since it might not be publicized. In the latter example, this countervalue target would raise significant audience costs because it endangers the life of the person, the person is a civilian target, and the person could represent anyone in society, which intensifies both the fear and sympathy response of the audience.

In the example of the military vehicle, the audience costs might be calculated differently if a military convoy was operating in hostile territory and all the vehicles were turned off and unable to drive, resulting in the soldiers taking fire and suffering casualties. However, it is still a counterforce target and may not garner the same level of audience costs that the CEO's disabled pacemaker example does. As George notes in *Forceful Persuasion*, the specific circumstances in each situation determine the success or failure of coercive diplomacy: there is no exact formula or mathematical equation to achieve successful coercion. Coercion is an art and there are critical factors that can contribute to success, but they are not solely determinate.

Key Terms

Cyberspace is composed of three terrains: the internet and all interconnected computers; the world wide web, that is the nodes accessible via URL; and, all other systems that exist but are not connected to the internet or web.[108] "Cyber conflict has changed only gradually over time; thus, historical lessons derived from past cases are still relevant today."[109] In the same way that ethics and international relations theory lessons from Thucydides still apply today, some 2400 years later, the lessons learned in the 1980s and 1990s cyberspace still apply today despite significant technological advancement.[110]

It is important to define the terms and concepts surrounding cyberspace, cyber conflict, and the issue of cyber coercion. 'Cyber warfare' is a recent term: Oxford English Dictionary gives its first use as 1994[111] and it is the oft-used catch-all term to refer any cyber conflict. The topic of cyber conflict has received widespread media attention only in the most recent decade or so; the overarching doctrine governing hostile cyber interactions in the 1980s was "information warfare." By the 1990s, it was considered "information operations" and the early aughts of the 21st century birthed

---

[108] Kello, Lucas. "The Meaning of the Cyber Revolution." *International Security*. Volume 38, Number 2, Fall 2013. p. 17.
[109] Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Washington DC: Cyber Conflict Studies Association, 2013.
[110] Moore's law measures exponential technological advancement in information systems. It is the observation that the number of transistors in a dense integrated circuit (chip speed) doubles every two years, and the cost is halved during this same timeframe. A contemporary interpretation is a focus on the increase of cores per die instead of simply clock speed, as was the original Moore's law. A core is a unit that runs in parallel with other cores; a die consists of several cores.
[111] Oxford English Dictionary. OED Online. June 2019. Oxford University Press. http://www.oed.com/.

widespread use of “cyber doctrine” and is the terminology that we continue to use today.[112]

In 1991, Dorothy Denning described cyber as a subcomponent of information warfare, which "...consists of offensive and defensive operations against information resources of a ‘win-lose’ nature.” Further, “[cyber] warfare is about operations that target or exploit information resources.”[113] At the time, the term “cyber warfare” was used to describe technology-based combat operations that leverages information technology to control and command systems in an effort to exert power over an adversary. While electronic warfare dates back several decades, the cyber aspects of this category of warfare have only been seen largely since the 1990s.[114]

Since the mid-1990s, the popular naming convention detailing different kinds of “cyber activity” have been categorized in several ways, as referenced above. Cyber conflict is when states and non-state actors “use offensive and defensive cyber capabilities to attack, defend, and spy on each other typically for political and other national security purposes.”[115] The terms “cyber conflict” and “cyber operations” are umbrella terms that include cyber war, cyberattacks, cyber exploitation, and cybercrime. For purposes of this research, cyber warfare will be defined as the state’s use of technology for its offensive or defensive strategy to control, destroy, or disrupt an

---

[112] Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Washington DC: Cyber Conflict Studies Association, 2013.
[113] Denning, Dorothy. *Information Warfare and Security* (Reading, MA: Addison-Wesley Longman, 1999), 21.
[114] Martin Libicki. *What is Information Warfare.* Government Printing Office, 1995. Page 7.
[115] Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Washington DC: Cyber Conflict Studies Association, 2013.

adversary's computer or network resources and systems in both the physical and nonphysical realms. Since the ramifications are “heavily damaging and destructive, similar to the effects achieved with traditional military force, [it is] considered to be an armed attack. An act of war that is mediated in full or part through cyberspace.”[116]

According to Herb Lin, "Cyberattacks refers to the use of deliberate activities to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting through these systems or networks.”[117] Conversely, "cyber exploitation" refers to the deliberate activities designed to penetrate computer systems or networks used by an adversary for the purposes of obtaining information resident on or transiting through these systems.[118] Under the umbrella of cyber operations, cyber espionage and cyber monitoring for intelligence purposes are activities authorized under intelligence law, and outside the scope of this research. Similarly, cybercrime is outside the parameters of this research since that is the purview of law enforcement. The last key component of the cyber environment is cybersecurity and how the state and non-state actors can use cybersecurity practices to help their offensive, defensive and coercive strategies.[119]

Since 2000, "the Internet has become a general-purpose technology that contributed some $4 trillion to the world economy in 2016 and connects nearly half the

---

[116] Healey, Jason. *A Fierce Domain: Conflict in Cyberspace 1986-2012*. Washington DC: Cyber Conflict Studies Association, 2013.
[117] Lin, Herb. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* 94, No. 886. Summer 2012. p. 518
[118] Lin, Herb. "Cyber Conflict and International Humanitarian Law." 2012. p. 518
[119] Kello, Lucas. "The Meaning of the Cyber Revolution." *International Security*. Vol 38, Num 2, Fall 2013. p. 17

world's population."[120] As society grows ever more reliant upon information technology and communications, the development of cyber network operations has emerged as a possible means of waging war. "... [A] key stated fear is [cyber] warfare, or sneak electronic assaults that could crash power grids, financial networks, transportation systems and telecommunications, among other vital services."[121] Historically, cyber threats have been generally viewed as acts of terrorism and consequently have been managed as such. Because the risks and potential for damage is vastly more increased, as the proliferation of and reliance on cyber networking increases, frequent attacks are more likely to occur in the form of cyber coercion or cyber warfare versus a physical offense.[122]

---

[120] Nye, Joseph. "Deterrence and Dissuasion in Cyberspace." *International Security,* Vol. 41, No. 3. Winter 2016/2017. p. 44

[121] Wolf, Jim. "U.S. Draws Attention to Information Warfare Threat." December 26, 2000. http://www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=004ITd. Accessed March 2, 2016.

[122] However, squirrels and others of the animal kingdom remain a significant threat to physical critical infrastructure due to their destruction of power cables and other associated cabling as has been widely noted. One such observation is captured in Gallagher, Sean. "Who's Winning the Cyberwar – the squirrels, of course." *Ars Technica*, January 16, 2017. Found at: https://arstechnica.com/information-technology/2017/01/whos-winning-the-cyber-war-the-squirrels-of-course and accessed on November 27, 2020.

Types of Cyber Attacks

What is a cyberattack? [123]

Examples of common cyberattacks include: Denial-of-Service (DoS), Malware (Trojans, Worms, Destroy data, Steal data, Poison data), phishing and spear phishing, website defacement and data breaches. These are described below.

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, systems are unable to complete legitimate requests and users cannot send nor receive information. Attackers can also use multiple compromised devices, sometimes thousands and often called botnets, to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.[124]

Malware

Malware is a term used to describe malicious software, including spyware, ransomware, trojans, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a malicious link or downloads email attachment that then installs risky software. Once inside the system, malware can do the following:

---

[123]The following list is compiled from various sources including the following: Cisco Products. "What are the Most Common Cyber Attacks?" Located at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html and accessed on November 6, 2019 and Kaspersky. Located at https://usa.kaspersky.com/resource-center/threats and accessed on November 6, 2019.

[124] Cisco Products. "What are the Most Common Cyber Attacks?" Located at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html and accessed on November 6, 2019

Blocks access to key components of the network (ransomware)

Installs malware or additional harmful software

Covertly obtains information by transmitting data from the hard drive

Disrupts certain components and renders the system inoperable

Trojan

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include:

Deleting data
Blocking data
Modifying data
Copying data
Disrupting the performance of computers or computer networks

Unlike computer viruses and worms, Trojans are not able to self-replicate.

Worms

Worms are a type of malware that replicates across networked computers independent of human interaction. Typically, a worm's purpose is to consume bandwidth and use up computing resources.

Destroy data

Destroying data has multiple negative consequences. The most obvious is that data is missing and cannot be used for assessment. However, missing data can also significantly change the outcome of machine learning models, change the boundaries of models, and reduce the accuracy in evaluating large datasets.

Steal data

Stealing data is when an adversary gains access to a computer system to copy data and send it to a computer controlled by the adversary. In this case, the original data is not altered, it is simply copied and sent out of the original network to one controlled by an adversary.

Poison data

Poisoning data is when an adversary is able to inject bad data into a computer system and/or database. With the rise of machine learning and artificial intelligence, more systems are relying on data models to understand large datasets in data science. Injecting false data into the training pool for data models can result in serious negative consequences, move the model's boundaries, and result in significant drop in accuracy of results.

Phishing and spear phishing attacks

Phishing is an email-borne attack based on sending fraudulent communications that

appear to come from a reputable source. The goal is to trick the recipient to disclose sensitive data like credit card and login information or to click a link that installs malicious malware on the victim's machine. Phishing is an increasingly common cyberthreat. Spear phishing is a more sophisticated version where the attacker learns about the victim and then pretends to be a trusted associate.

Website Defacement

Website defacement refers to the involuntary change of appearance of a website. It can include pictures and/or words placed on a defaced website and can be in a graffiti style or replace the style of text for the purposes of misleading the audience.[125]

Data Breaches

A data breach is a theft of data by a malicious actor using one or more methods listed above. Motives for data breaches include cyber coercion, crime (i.e. identity theft), and espionage.[126]

Table 5. shows which types of cyberattacks were used for each dyadic case.

[125] TrendMicro. "Website Defacement." Located at: https://www.trendmicro.com/vinfo/us/security/definition/website-defacement

[126] The motives of crime (e.g. identity theft) and espionage are outside the focus of this research.

Table 5: Typology of cyberattacks types and what was used against Sony and Estonia

Types of Attack[127]	Used against Sony	Used against Estonia
Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks to cause the failure of victim communications	Yes	Yes
Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks to cause the failure of media communications and limit information	No	Yes
Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks to cause economic failure	Yes	Yes
Phishing and spear phishing attacks	Yes	No
Malware attack	Yes	No
Defacing websites	Yes	Yes
Stealing and leaking data	Yes	No

[127] This is to illustrate the different types of attacks used. There is no argument that the type of attack matters as much as the information gleaned and to what extent that information is made public or exposed.

The Coercive Use of Cyber Actions

Offense-Defense Theory and Cyber

Offense-defense theory attempts to discern how technology affects the likelihood of conflict. The intersection of offense-defense theory literature with how specific technology developments affect the likelihood of war is an important to examine. As assembled by scholars Robert Jervis, George Quester and Stephen Van Evera,[128] the offense-defense theory, at its most basic, says that when states believe they can conquer one another more easily, war will be prevalent. Offense-defense theory refines the Realist argument and, using it as a lens to approach the usefulness of cyber debate, serves further to clarify the position of various theorists and academics as well as provide a different perspective from which to view the cyber debate. Offense-defense theory typically leans toward favoring the defensive posture, however conventional wisdom for cyberspace argues that due its wide attack surface, multiple avenues to exploit vulnerabilities, and various cyber characteristics tip the balance in favor of being offense dominant.[129] A small number of prominent cyber-focused scholars disagree with this conventional wisdom and believe it is a nuanced balance where high value target attacks can be extremely difficult and costly, where quality of target matter more than quantity and that

---

[128] Quester, G. H. (1977). *Offense and Defense in the International System*. New York: John Wiley & Sons. Jervis, R. "Cooperation Under the Security Dilemma." World Politics 30(2): 1978. p. 167-214. Van Evera, Stephen. "Offense, Defense and the Causes of War." *International Security*, Spring 1998, Vol. 22, No. 4. p. 5-43

[129] This conventional wisdom is demonstrated in the following: Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (Fall 2013), p. 7–40; Lieber, Keir. "The Offense-Defense Balance and Cyber Warfare," in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies.* Monterey, CA: Naval Postgraduate School, 2015. p. 96–107.

determining the offense-defense balance may be highly dependent upon the specific dyadic interaction.[130] The basic underlying cause for the rapid offense–defense cycle of cyberweapons is that cyberspace is more malleable.[131] Lindsay and Gartzke nicely distill the various competing factors involved in determining offense-defense balance in cyberspace, noting that:

> Widespread belief that offense is easier than defense in cyberspace, that stronger states are increasingly vulnerable while weaker actors are increasingly empowered, and that the anonymity of cyber operations precludes effective deterrence leads many to argue that cyberspace brims with unprecedented, even revolutionary dangers. Yet national security officials, defense firms, media pundits, and a burgeoning private cybersecurity industry all have incentives to exaggerate the threat, while the extreme secrecy of cyber operations complicates sober assessment. [132]

Offense-defense theory also calls into question the various definitions offered by scholars in the international relations (IR) field. There are four major characterizations accepted in IR literature concerning offense-defense. Of those four, three specifically focus, in part, on the integration of technology in military engagements. The fourth depends upon military skill and ability which, when viewed through the lens of cyber, supports the notion that offense-defense theory is directly related to determining the usefulness of cyber as a tool of coercive diplomacy. Briefly, the competing definitions

---

[130] This small number of scholars includes: Rid, Thomas. "Cyber War Will Not Take Place." *The Journal of Strategic Studies*, Vol 35, No. 1. p. 28; Gartzke, Eric and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace." *Security Studies*, 24:316–348, 2015.

[131] Smeets, Max. "A matter of time: On the transitory nature of cyberweapons." *Journal of Strategic Studies*, 2018: 41:1-2, 6-32. p. 12.

[132] Lindsay, Jon and Erik Gartzke. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." In Kelly M. Greenhill and Peter J. P. Krause, eds., *The Power to Hurt: Coercion in Theory and in Practice.* p. 179-180.

are as follows:

1. Jervis, Quester and Lynn-Jones are of the same opinion and narrow definition that offense-defense theory is determined by the choice of technology available to states. In addition, the balance is also affected by one states' investment in offense in order to counteract a rival's defense interests.[133]
2. Kaufman and Glaser see that offense-defense balance is best analyzed by addressing a particular pair of states and then investigating "the ratio of the cost of the forces that the attacker requires to take territory to the cost of the defender's forces."[134] Gilpin agrees with Kaufman and Glaser, writing, "the defense is said to be superior if the resources required to capture territory are greater than the value of the territory itself; the offense is superior if the cost of conquest is less than the value of the territory."[135]
3. Van Evera offers an extremely broad definition that incorporates technology, military doctrine, military posture, geography, social order, collective security systems, alliances and a history of balancing or band wagoning.[136]
4. Biddle asserts that the success of offensive action is due to the offensive state's

---

[133] Jervis, Robert. "Realism, Neorealism and Cooperation: Understanding the Debate." *International Security*, 1999, Vol. 24, No. 1. See also, Glaser, Charles. "Realists as Optimists: Cooperation as Self-Help." *International Security*, 1994/95, Vol. 19, No. 3; Lynn-Jones, Sean. "Does Offense-Defense Theory Have a Future?" Based on a talk delivered to the Research Group in International Security at McGill University on October 20, 2000. Held by the National Library of Quebec.
[134] Glaser, Charles and Chaim Kaufmann. "What is Offense-Defense Balance and Can We Measure It?" *International Security*, Spring 1998, Vol. 22, No. 4. p. 46.
[135] Gilpin, Robert. *War and Change in World Politics*, Cambridge University Press, 1981. p. 63.
[136] Van Evera, Stephen. "Offense, Defense and the Causes of War." *International Security*, Spring 1998, Vol. 22, No. 4.

comprehension of the adversary's center of gravity, its ability to attack that center and the adversary's failure to prevent an attack.[137]

Offense-defense theory holds that, when defensive capabilities are easier to achieve than offensive, then war is less likely and security is strengthened.[138] With the introduction of cyber vulnerabilities, offensive and defensive capabilities of an adversary must be re-addressed. For purposes of this research Robert Jervis' definition, will be used. Expanding on his outline, this explanation states that the two fundamental variables that guide the theory are:

1. Offense-defense balance: the judgment on whether conquering territory or defending it will be most successful.
2. Offense-defense differentiation: determining whether forces and capabilities that provide for offensive measures are different than those which support defensive action.[139]

In cyber statecraft, a common refrain is that offense just has to succeed once; defense has to be right all the time. This idea is part of the calculation in determining the conventional wisdom that in cyberspace offense is dominant. "Cyberattacks are cheap,

---

[137] Summarized in Lynn-Jones, Sean. "Does Offense-Defense Theory Have a Future?" Based on a talk delivered to the Research Group in International Security at McGill University on October 20, 2000. Held by the National Library of Quebec.
[138] Walt, Stephen. "International Relations: One World, Many Theories." *Foreign Policy*, Spring 1998. p. 31.
[139] Jervis, Robert. "Cooperation under the Security Dilemma." *World Politics*, January 1978, Vol. 30, No. 2. p. 187-194.

whereas cyber defense is expensive."[140] According to Libnicki, "if the offense-defense curves continue to favor the offense, one could argue that either the potential damage from a cyberattack would be unacceptable or the resources that must be spent on defense are unaffordable."[141]

Van Evera sees technology as favoring either offensive or defensive posture depending on how an individual state wishes to employ it.[142] An important component of state decision making and the means-ends relationship are the assumptions made about the relative strengths of offense and defense that directly impact the penchant for conflict.[143] Clearly, if a state believes it holds offensive supremacy, that is, it expects conflict to be quick and victorious, then it will be more inclined to enter into conflict than a state that holds the opposite view.

Slayton looks at cyber through the lens of offense-defense theory and argues that the idea of offense dominance in cyberspace is flawed. She asks important questions about the offense-defense balance in cyberspace and provides a framework for analyzing it in cyberspace operations. However, she neglects basic characteristics about networked systems and underestimates industrialized state's reliance on the internet for daily functioning. Slayton notes "…although digital industrial control systems (ICS) have

---

[140] Lieber, Keir. "The Offense-Defense Balance and Cyber Warfare," in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies.* Monterey, CA: Naval Postgraduate School, 2015. p. 96.
[141] Libnicki, Martin. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009. p.61.
[142] Van Evera, Stephen. "Offense, Defense and the Causes of War." *International Security*, Spring 1998, Vol. 22, No. 4.
[143] Jervis, Robert. "Cooperation under the Security Dilemma." *World Politics*, January 1978, Vol. 30, No. 2.; Van Evera, Stephen. *Causes of War: Power and the Roots of International Conflict.* Ithaca, NY: Cornell University Press, 1999.

been exploited by cyberweapons, achieving a desired physical effect is much more expensive than simply exploiting software vulnerabilities."[144] However, this is not always true.

As recently seen at an Oldsmar, Florida water plant, a bad actor accessed the plant's software and made seemingly minor changes in the acceptable water treatment levels, resulting in potentially catastrophic physical repercussions by poisoning the water supply.[145] Luckily, an employee on duty at the time watched the hack happen and was able to alert and override the change, but the timing was serendipitous. A more meticulous bad actor hacker could have accessed the system outside of business hours, therefore avoiding detection. What may have been considered prohibitively expensive when Slayton wrote in 2016, is no longer true in 2020. Lindsay offers that

> ...conventional wisdom holds that a multitude of technical factors favor offense over defense in cyberspace and that the difficulty of attribution undermines the credibility of deterrence; therefore, weaker actors can attack the control systems of superior adversaries to achieve levels of physical disruption possible previously only through kinetic bombing.[146]

Farwell and Rohozinski offer that "Clausewitz believe that in warfare, the advantage rested with the defense." Cyber reverses that equation. It also offers the potential to build the fog of war through the ability to effect disruption, deception,

---

[144] Slayton, Rebecca. "What is the Cyber Offense-Defense Balance?" *International Security* 41:3. Winter 2016/2017. p. 91.
[145] Mathews, Lee. "Florida Water Plant Hackers Exploited Old Software And Poor Password Habits." *Forbes*, February 15, 2021. Located at: https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poor-password-habits/?sh=3514b8b5334e and accessed on February 21, 2021
[146] Lindsay, Jon R. "The Impact of China on Cybersecurity." *International Security*, Vol. 39, Num 3. p. 29.

confusion and surprise."[147] The global diffusion of technological means and instruments allows any state to create sophisticated networking and communications abilities, thus increasing its defensive potential but also increasing potential vulnerabilities for an adversary to exploit.

Akin to other aspects of cyberspace operations, assessing the offense-defense balance in cyberspace is tricky because unlike conventional arms that can be seen, quantified, and its capabilities analyzed, the secretive nature of cyberspace offensive capabilities adds to the difficulty in judging the offense-defense balance. Defensive capabilities of an adversary may be easier to unearth by penetration testing, port scanning, and other red team techniques as well as the adversary's national publications identifying their defensive strategies, critical infrastructure and public cybersecurity budget documents. These resources do not exist for offensive cyber since public declaration would render offensive tools moot. As Nye notes, "though information warfare is not new, cyber technology makes it cheaper, faster, and more far-reaching, as well as more difficult to detect and more easily deniable."[148] These factors contribute to the proliferation of cyber capabilities and the murkiness of determining the offense-defense balance in cyber statecraft. Further, they tend to favor the offensive use of cyber capabilities, which is well-suited for cyber coercion.

---

[147] Farwell, James P. and Rafal Rohozinski. "The New Reality of Cyber War." *Survival*, Vol 54, Num 4, p. 114.
[148] Nye, Joseph. "Information Warfare versus Soft Power." *Project Syndicate*, Prague, May 2017.

The Anarchical World, the United Nations, Power, Laws, Norms and Coercion

Why are states and non-state actors allowed to threaten to harm or use force via cyber capabilities against other states and non-state actors? Is that simply a function of the anarchical world of self-help or are there international institutions that can intervene? What is the role of the United Nations in cyber statecraft, if any? What does assistance for cyberattacks and cyber coercion look like in a self-help world?

Understanding the limitations and assistance available for states and non-state actors suffering cyberattacks and cyber coercion in an anarchical world is integral to understanding the calculation of an aggressor state or non-state actor using cyber capabilities to achieve a political goal. For example, if there is no enforcement mechanism to punish the aggressor or no mutual aid agreement to assist a victim, then an aggressor is free to pursue cyber statecraft unrestricted as opposed to other coercive means and threats where they may be restricted.[149] This assumes, however, that the Realist, anarchical worldview is prevailing; there is a competing perspective by liberal institutionalists that increasing cooperation and aid among states through international institutions and agreements can lead to a positive outcome.

It is useful for the discussion on cyber coercion to understand these two

[149] For other types of capabilities in conflict there exist various international treaties and/or international institutions that play a role in "refereeing" their use, to varying degrees of success. Two prominent examples of these treaty restraints are: the Chemical Weapons Convention (CWC) and the Mine Ban Convention against the use of landmines, etc. The international community has codified via treaty, that some types of weapons and/or how they are used against specific populations should not be allowed as well as providing for mutual aid if, e.g., someone threatens the use of chemical weapons under the CWC. Of course this is for states opting into the treaty, but it also speaks to the formation of norms around a particular capability.

competing worldviews and their real-world implications for a state or non-state actor to choose cyber coercion to achieve a political end. One could argue that these differences in worldviews are emblematic of the differences seen in the approach to cyberspace between members of the European Union and other significant powers in the cyberspace world. That is, EU member states have pushed for international agreements on norms of behavior in cyberspace, a charter to unite under common principles respecting international law in cyberspace and efforts to create greater stability through a reduction in cyberattacks. Meanwhile, other significant powers in cyberspace have declined to join these efforts reflecting an unwillingness to artificially limit options for using offensive and defensive cyber statecraft.

To better understand the theoretical underpinnings of these differing world views we turn to a debate in the mid-1990s. Theories that rely upon the possibility of conflict reduction through the formation of international institutions are inherently flawed. This is the argument put forth by the preeminent scholar of Offensive Realism, John Mearsheimer. Disagreeing, Robert Keohane offers great optimism about the benefits that nations reap from participating in the international institutions, writing that

> "when states can jointly benefit from cooperation…we expect governments to attempt to construct such institutions. Institutions can provide information, reduce transaction costs, make commitments more credible, establish focal points for coordination, and in general facilitate the operation of reciprocity.[150]

Juxtaposing Mearsheimer's Realist view[151] with Robert Keohane's utilitarian,

[150] Keohane, Robert and Lisa Martin. "The Promise of Institutionalist Theory." *International* Security, Vol. 20, No. 1 (Summer, 1995): 42

[151] Mearsheimer, John. *The Tragedy of Great Power Politics*, 2001. See also, John Mearsheimer

rationalistic, Institutionalist view[152] provides contrasting accounts of the usefulness of international institutions as means to reduce conflict. This contrast can be applied to the study of cyber statecraft as a means to view different perspectives when examining an aggressor's choice to employ cyber capabilities for coercive purposes or a state's choice to enter into, or refrain from, international agreements on behavior in cyberspace.

"According to Realist theory in political science, states exist in an anarchical international system and must therefore rely on self-help to protect their sovereignty and national security."[153] When applying this to cyber statecraft, Realism dictates that each state should only rely on itself to deter and defend against cyberattacks and that international cooperation will not protect a victim state from a determined aggressor.

Rebutting that theory is the idea that cooperation through international institutionalism, where the state has shared common interests, can provide a pathway and powerful incentive for states to cooperate, as well as compete, to avoid conflict. States seek to maximize their nation's welfare, military security, and power. In an increasingly integrated world, states are constrained to work together for mutual advantages. The cyber realm is an excellent example where states are strongly motivated to work together to reduce the threat of cybercrime and cyberwarfare. Failure to do so would incur significant costs and would reduce their standard of living, and thus their long-term

---

"The False Promise of International Institutions," *International Security,* Vol. 19, No. 3 (Winter, 1994-1995), p. 5-49

[152] Keohane, Robert and Lisa Martin. "The Promise of Institutionalist Theory." *International* Security, Vol. 20, No. 1 (Summer, 1995): 39. See also, Keohane, Robert. *After Hegemony*. Princeton, NJ: Princeton University Press. 1984.

[153] Quoted in Sagan, Scott. "Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb" *International Security*, Vol. 21, No. 3. p. 57. Original idea from Kenneth Waltz, *Theory of International Politics*. New York: Random House, 1979.

viability. However, as noted above, we see some states opt out of these international agreement efforts and it is important to understand how they may view them differently from those proposing and promoting these agreements.

Arguably, "…'institutionalist' theories [are] largely a response to realism and …directly challenges realism's underlying logic."[154] Mearsheimer's assumptions are as follows: the world exists in anarchy; states seek survival; states possess offensive military capability; states will act rationally; and, states are uncertain about one another's intentions and it is this uncertainty that drives the power maximizing desire.[155] Keohane's argument against the last assumption is that although international institutions may not always reduce uncertainty and transaction costs and therefore they may not necessarily strengthen cooperation, the possibility of increased information sharing through these bodies exists so that undermines Mearsheimer's last basic assumption.

Mearsheimer's logic stems from the realist paradigm, naturally on the systemic level, and is highly pessimistic about the role that international organizations can play in reducing conflict. He claims "…institutions have minimal influence on the state behavior, and thus hold little promise for promoting stability in the post-Cold War world,"[156] but he systematically disregards the constructive aspects of international institutions. When applied to cyberspace, the usefulness of international institutions need

---

[154] Mearsheimer, John. "The False Promise of International Institutions." *International Security*, Issue 19, No. 3. Winter 1994/1995. p. 7.
[155] Mearsheimer, John. *The Tragedy of Great Power Politics.* W.W. Norton & Company: New York, 2001.
[156] Mearsheimer, John. "The False Promise of International Institutions." *International Security*, Issue 19, No. 3. Winter 1994/1995. p. 7.

not be completely discounted when looking at how to reduce cyber conflict in the international system through cooperation or coercion; the attempts in recent years to create international institutions to achieve a reduction in cyber conflict are a testimony to their burgeoning influence in the cyber realm. That being said, Mearsheimer's insight may explain why several significant cyber actors refuse to sign onto international cyber agreements restricting cyber activity.

Mearsheimer contends that although international institutions may be a factor in forming cooperation among states, "…there is little evidence that they can get great powers to act contrary to the dictates of realism."[157] This criticism appears to be shared by states that have thus far rejected the appeals to enter into an international agreement that will restrict their own use of cyber capabilities while having zero effect on their adversaries. Since international institutions lack the authority to enforce cyber-focused agreements, states and non-state actors may decide that employing cyber capabilities may be beneficial to achieve their goals and may not want to artificially limit their ability to exercise these capabilities.

Keohane seeks to challenge the assumption that one state can never be certain about another's intentions[158] and sees that the "logic of institutionalist theory, with its focus on the informational role of institutions, appears solid."[159] Keohane posits that,

---

[157] Mearsheimer, John. *The Tragedy of Great Power Politics.* W.W. Norton & Company: New York, 2001. p. 364.

[158] This is why George's condition of "Clear Objective" is so important to successful coercive diplomacy; ambiguity of intentions between states can introduce unnecessary friction. .

[159] Keohane, Robert and Lisa Martin. "The Promise of Institutionalist Theory." *International* Security, Vol. 20, No. 1 (Summer, 1995): 51.

through the use of international institutions, states may be able to increase and facilitate communications and secure more information, therefore affording the opportunity to convey — and divine — future intentions. This is one method by which states can increase cooperation, decrease cheating, comprehend the objectives of another state and perhaps alter its own behavior in light of another states aims or willingness to work together.[160] Increased sharing of information through institutions can provide insight into others' intentions and lead to policies that maximize potential instead of policies that assume a worst-case scenario (given an uncertain, anarchic world) and therefore are unable to maximize utility.[161] Cyberspace has been an anarchical environment since its inception and is plagued by the unknown intentions and capabilities of adversaries. Several international efforts have attempted to build consensus and cooperation over the past twenty years, but only in recent years has there been slight progress on this front.

In cyber statecraft, there have been several attempts to create venues for cooperation and agreement. One example is the 2018 Paris Call for Trust and Security in Cyberspace, which was an attempt to unite under common cyber behavior principles to govern cyberspace and reaffirm the applicability of international law, IHL and the UN Charter in an effort to create greater stability in cyberspace. The Paris Call was a pledge to unite under nine principles to provide greater international security in cyberspace. Several local and federal governments signed on as well as private sector and civil society participants. However, at the 2019 NATO CCDCOE CyCon, the leading cyber

---

[160] Keohane, Robert and Lisa Martin. "The Promise of Institutionalist Theory." *International* Security, Vol. 20, No. 1 (Summer, 1995): 44
[161] Ibid. p. 44.

defense conference in Europe, the utility of the Paris Call was debated because several major actors in cyber statecraft, such as Russia, China, India and the United States, refused to sign on to the Paris Call. This resulted in scholars calling into question the power of its influence and repeating the criticism endemic to international institutions: the lack of enforcement mechanisms.[162]

The debate between Mearsheimer and Keohane is used as an example because it exemplifies the debate happening across the world on how best to deal with the challenges of cyber statecraft. Should states seek to restrain behavior by international agreements that are difficult to enforce but can serve to limit some bad behavior in cyberspace? Or, it is in a state's self-interest to refuse to enter into international agreements so that one may operate in cyberspace unconstrained?

Cyber Statecraft: International Norms

Despite the fact that the internet has been popularly used since the 1990s, and widely used globally since the early 2000s, only in recent years has the international community coalesced seriously around formalizing norms for behavior. The "topic of ICTs in international security is not new in the United Nations, it has been on the agenda of member states since 1998"[163] and the UN has convened six Groups of Governmental

[162] Firsthand account from this researcher who was an attendee at the 2019 NATO Cooperative Cyber Defence Centre of Excellence Cycon in Tallinn, Estonia, May 28-31, 2019.
[163] Izumi Nakamitsu, Under-Secretary-General and High Representative for Disarmament Affairs, United Nations, remarks presented at "Deciding on the Rules of the Road for Cyberspace: The Who, What, Where, When, How" at the Institute of International Cyber Stability, June 9. 2020.

Experts (GGE) since 2004 to examine how ICTs impact international security. And yet these norms are an evolving process, with several still being codified. The idea of cyber norms was further explored during the 2009 NATO Cyber Conference in Tallinn, Estonia, but the initial norms of behavior in cyberspace were not widely agreed upon until 2015.[164] And, like any system of international norms, these cyber norms must be agreed to by all willing participants. The cyberspace norms of behavior continues to be an evolving conversation in the international community with the formation of the 2018 Paris Call for Trust and Security in Cyberspace, the formation of the 2018 United Nations Group of Governmental Experts (GGE) on Advancing Responsible State Behavior in Cyberspace, consisting of 25 Member states, and the creation of the 2018 United Nations Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) that was open to all UN Member states.

In March 2021, in a first for the OEWG, the UN Member states agreed to endorse a report on recommendations to advance peace and security in cyberspace. This marks the first time all Member states have agreed to a report to advance the norms surrounding state behavior toward cybersecurity; however, of note, the report and subsequent endorsement includes "…11 voluntary, non-binding norms of responsible State behavior

[164] Those non-binding norms, as adopted by the UN GGE in 2015, are: (1) 'States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions' (norm G), and (2) 'States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty' (norm H).

and [it] recognized that additional norms could be developed over time." [165] While an excellent first step, to echo Mearsheimer's criticisms of liberal institutionalism, the fact that it is not legally binding and that there is a lack of an enforcement mechanism means that some Member states may have agreed with no intention of abiding by it. Iran decided to 'disassociate' from it, citing 'unacceptable content' which did not block consensus on the report, but is a move rarely seen at the UN. It may provide Iran a future excuse not to abide by the recommendations in the report. "In the end, no country was fully pleased with the contents of the report. Iran even went so far as to "disassociate" itself from it, given "unacceptable content." While it did not ultimately block consensus on the report, disassociation is an uncommon UN practice which provides Iran with some basis to claim it is not bound by the report's conclusions. Specifically, "…the Islamic Republic of Iran is not obliged with any term, content, paragraph, conclusion, and recommendation of the report that is not in line with its principled positions."[166]

That being said, Keohane would argue that this first agreement provides the foundation for future international cooperation, an ability to grow consensus and share information, and venue for future cybersecurity negotiations among states. Engaging in cyber coercion may sometimes be the choice between maximizing one's power or sacrificing that opportunity to be part of a cooperative team. Mearsheimer argues that the

---

[165] United Nations General Assembly: Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. *Final Substantive Report*, March 10, 2021. Located at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[166] United Nations General Assembly: Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. *Compendium of Statements in Explanation of Position on the Final Report.* March 8-12, 2021. p. 45 Located at: https://undocs.org/pdf?symbol=en/A/AC.290/2021/INF/2

former will prevail, but as this first endorsement of the OEWG report by the Member states shows, there is room for Keohane's theory to prevail.

Cyber Statecraft: International Law

To properly analyze cyber coercion actions, it is necessary to understand the larger cyber operations framework and how it interacts with international law. The Tallinn Manual[167] lists eight factors to "identify cyber operations that are analogous to other non-kinetic or kinetic actions that the international community would describe as uses of force: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality."[168] Meanwhile, Koh notes: "We must distinguish between hacking, network exploitation and network attack. We must translate the "spirit" of existing international law to the new tools of 21st century war."[169]

In cyberspace and computer network operations, there are a number of competing and overlapping factors, norms and laws against targeting civilian infrastructure and the private sector. However, the soft target private sector and civilian infrastructure is routinely targeted, as it was in both case studies in this research. "The use of cyberattack

[167] The Tallinn Manual on the International Law Applicable to Cyber Warfare is a continuously-updated collection of expert opinions of a number of academics and practitioners operating in their personal capacity. It is a is a product of the NATO Cooperative Cyber Defense Centre of Excellence but does not reflect the views of the NATO CCD COE or NATO and is not meant to reflect NATO doctrine. Original volume: Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.
[168] Tallinn Manual. p 48-51.
[169] Koh, Harold Hongju. "The Emerging Law of the 21st Century War." *The Brookings Institute*. Breyer Lecture presentation, April 1, 2016.

is governed by "jus in bello" or the Law of Armed Conflict. These laws are derived from international conventions and treaties (such as the Hague and Geneva Conventions) and from customary international law. They set forth rules that govern the use of force during armed conflict."[170] There are three principles from the Laws of Armed Conflict that apply to cyberspace and assist in judging the legality of cyber statecraft actions. These are:

1. The principle of distinction requires attacks to be limited to legitimate military objectives and that civilian objects shall not be the object of attack. Article 23 of the Hague Convention, for example, forbids belligerents "to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war."[171]
2. The principle of proportionality requires that the use of force in self-defense must be limited to that which is necessary to meet an imminent or actual armed attack and must be proportionate to the threat that is faced. Attacks on a military objective which cause incidental loss of life or injury to civilians or damage civilian property, in excess of that needed to obtain concrete and direct military advantage are prohibited.[172]
3. The principle of discriminate attack prohibits attacks that cannot reasonably be limited to a specific military objective, and which are indiscriminate or haphazard in their inclusion of civilian targets. Article 27 calls for belligerents

[170] Lewis, James A. "A Note on the Laws of War in Cyberspace." *Center for Strategic and International Studies,* April 2010. p. 2.
[171] Ibid.
[172] Ibid.

> to take all necessary steps to avoid damage to "buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes."[173]

Under the Laws of Armed Conflict, in cyber statecraft, an aggressor must assess the civilian collateral damage potential before engaging in an action, the same operational process that is required for kinetic actions. "The goal of the protections for civilians found in the laws of war is not to shield them from the dangers of military operations but to avoid capricious attacks undertaken solely to harm civilian targets."[174] However, also akin to the kinetic realm, these laws are only adhered to by willing participants; if a pariah state or non-state actor wishes to engage in destructive cyber statecraft behavior targeting civilian entities, they do, as is described in both case studies in chapters four and five.

The Laws of Armed Conflict and cyber norms and their application to cyber statecraft are only as good as when they are widely-adopted, used and operationalized. There have been a number of global cyberattacks that violate these laws and norms, and those attacks are often from states that also consistently violate other international laws and norms, such as Russia and North Korea.[175]

How useful are cyber norms and the application of international law to

---

[173] Ibid.
[174] Ibid.
[175] As repressive regimes, Russia and North Korea have violated international norms and laws on a variety of issues ranging from international sanctions violations to human rights to extrajudicial murder.

cyberspace? If the state agrees with the norm framework and cooperates (good international institutionalists) but a state that does not buy into the cooperation agreement then attacks (the realist, self-help world of anarchy) then does the institutionalist agreement matter? It becomes an agreement among friends, and some may see that agreement as limiting when in conflict with a state that does not agree to these limitations.

On March 5, 2020, for the first time in the history of the Security Council, Estonia raised the issue of cybersecurity. According to the President of Estonia, Kersti Kaljulaid:

> "Our goal [in going to the UN Security Council] was to start creating the new normal; that if a country comes under cyberattack, then they will have at the Security Council a place to report about it, complain about it, and ask other countries to react, take positions, and maybe one day also take action. …We still don't have a clear understanding of how we are able to protect our sovereignty [in cyber].[176]

Although the United Nations noted in June 2020 that the subject of cyber (aka ICTs) has been part of the UN international conversation since 1998, serious attention has only coalesced around the subject in recent years. Countries like Estonia, who suffered significant cyberattacks in 2007, were forced to confront the importance of cybersecurity needs and became an early adopter of best practices to create a secure digital environment in the country. As noted by the Estonia President at an international conference on cyber stability: "When we finally had a really good conference on the 8th of May in the UN Security Council, somebody quipped that it was probably a small step for Estonia but a

[176] President of Estonia, Kersti Kaljulaid, remarks presented at "Deciding on the Rules of the Road for Cyberspace: The Who, What, Where, When, How" at the Institute of International Cyber Stability, June 9. 2020.

big step for the world and I have to say that it doesn't exactly sound modest if I confirm but we felt a little bit this way. Our point has been proven."[177]

This section provided the greater context to fully understand the environment in which cyber coercion occurs, the different perspectives on how to approach the issue of cyber statecraft and how different powers view constraints on employing these cyber capabilities. Equipped with a better understanding of the constraints, or the lack thereof, in cyber statecraft, and how the strategic choices of state actors to conduct cyber coercion fits within the larger cyber operations framework, the next section proceeds to describe the argument of this research.

[177] President of Estonia, Kersti Kaljulaid, remarks presented at "Deciding on the Rules of the Road for Cyberspace: The Who, What, Where, When, How" at the Institute of International Cyber Stability, June 9. 2020.

Argument

When a state decides that they would like another state or non-state actor in the international community to change their behavior toward a particular issue, a state has several levers of power it can use to exercise to exert pressure. These levers range from diplomatic demarche to public embarrassment to economic sanctions to cyber coercion to kinetic action and a whole host of additional options in between. This research focuses on cyber coercion where the targets are soft, countervalue targets[178] in an open, democratic society, and identify and examine what variables contribute to determining a variety of victim responses.

Once a state or non-state actor has decided to engage in cyber coercion, it must design a strategy, choose targets, select the tactics and initiate the operation. There are a number of variables that go into this calculation. In examining previous coercive diplomacy dynamics, George identified seven conditions that favor coercive diplomacy (Clarity of the objective, Strength of Motivation, Asymmetry of Motivation, Sense of Urgency, Adequate Domestic and International Support, Opponent's Fear of Unacceptable Escalation, and Clarity Concerning Precise Terms of the Settlement of a Crisis). However, for cyber coercion this set of variables must be expanded to include 1) financial costs for the victim, 2) audience costs for the victim,[179] 3) leadership

[178] Countervalue targets are those that do not pose an overt military threat and are most often defined as civilian population centers such as towns and cities, but also include non-military government targets. Conversely, counterforce targets are those that pose a military threat, and consist mostly of government and military personnel and military controlled geographic targets.
[179] Byman and Waxman in The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might refer to audience costs, but only in terms of a cautionary tale. They describe it as the problem of "*over*coercing" and may lead adversaries to "take risks it would otherwise

destabilization potential through targeting of leadership, and 4) the amount of pressure on leadership. These variables are defined in the following ways:

1) Financial costs for the victim – the actual financial costs incurred by the victim to include the cost of rehabilitating or replacing the hardware and software, rebuilding their network, legal costs associated with the ramifications from a cyberattack, the financial losses incurred from an inability to function for a period of time and any other financial ramifications stemming from the consequences of the cyberattack.

2) Audience costs for the victim – traditional audience costs refer to the consequences a leader incurs from their constituency if they escalate a crisis and then back down. "If a state backs down, its leaders suffer audience costs that increase as the crisis escalates. These costs arise from the action of domestic audiences concerned with whether the leadership is successful or unsuccessful at foreign policy"[180] For purposes of this research, which includes a commercial industry victim that is not beholden to a constituency, but instead to customers and business associates, that definition is expanded to include the reputation costs for the company in its dealings with various business associates and retaining customers. Further, this expanded definition is not only limited to the consequences of backing down and being unsuccessful at foreign policy like a state actor, but also includes all the consequences to its corporate reputation from engaging with, or ignoring, a cyber adversary.

---

avoid and to escalate a conflict in order to stay in power." Daniel Byman and Matthew Waxman. The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might. Cambridge: Cambridge University Press, 2002. p. 36-37.

[180] Fearon, James. "Domestic Political Audiences and the Escalation of International Disputes." *American Political Science Review*, Vol 88, No. 3, September 1994: 577-592.

3) Leadership destabilization potential through targeting of leadership – if leadership is specifically targeted in a cyber coercive act there can be a higher potential for leadership destabilization based on the nature of the attack against leadership. If leadership is targeted and the result is embarrassing or compromising information that is then revealed (either broadly or narrowly) leadership may have to step down or be relieved of duties. If leadership is undermined or punished during a cyber coercion negotiation, the victim's ability to bargain can be severely weakened and their ability to negotiate can be superseded by personal demands.

4) The amount of pressure on leadership – akin to specifically targeting leadership, the amount of pressure on leadership is a function of the nature of the cyberattack. That is, if the cyberattack paralyzes the victim for days or weeks and people are unable to work and unable to carry on their daily activities, the pressure on leadership will be high. Further, if there is a personal disparaging angle to the cyber coercion, the amount of pressure on leadership will be high. Conversely, if the nature of the cyberattack does not reach a level of high incapacitation nor deride the leadership nor significantly impact daily life, the leadership may feel low pressure to resolve the conflict.

The assumptions for this research are the following:

1) An aggressor seeks to change the behavior of the victim and that is why the aggressor is engaging in cyber coercion and not solely for the sake of being belligerent or destructive.

2) Through the use of advanced cybersecurity analysis best practices and leveraging private industry's unique aperture combined with Healey's Spectrum of State Responsibility and Sharp's Known Coercer plus Known Demand Standard, we can achieve sufficient attribution of an aggressor.

3) The aggressors in these case studies, Russia and North Korea, follow an essentially Realist understanding of the world – i.e. along the lines of Mearsheimer's belief of an anarchical world of self-help which contributes to their individual choices to engage in cyber aggression as opposed to working through a cooperative solution via an international institution.

This research argues that certain variables from George's list of seven conditions that favor coercive diplomacy matter more in cyberspace than others in getting a victim to change their behavior and misestimating those variables can lead to failure. Further, this research argues that audience costs and/or financial costs have significant consequence in altering a victim's behavior over time, but only when there is asymmetry of motivation and fear of escalation. Related, as described in the case studies in chapters four and five, targeting soft targets that suffer higher audience costs and higher financial costs compared with counterforce targets is a specific decision by an aggressor that may or may not contribute to changing a victim's behavior, depending on the aggressor's targeting choices. Lastly, that leadership destabilization may be a consequence of cyber coercion, and while it may not directly change a victim's behavior vis-à-vis the demand over time, leadership destabilization is an important consequence of cyber coercion.

Research Question

The primary research question of the dissertation is: what effect does the variation in coercive strategy, relative conditions that favor coercive diplomacy (i.e. to what degree does a cyber campaign satisfy the seven conditions listed by George) and an expanded set of additional variables have on victim responses to cyber coercive measures over time when the target choice focuses on soft, countervalue targets? For this dissertation, the dependent variable (DV) is how each victim responded to the threatening computer network operations (CNO) action, including if the victim response changes over time and it is measured by the reported actions taken by the victims. Previous literature only looked at the result in the binary of success or failure in changing a victim's behavior and was artificially restrictive to the immediate temporal value; this expands the definition of effective coercion from a binary understanding to a spectrum of five and extends the time range across three temporal values. The options for the DV values comprise an escalation spectrum and include: [181]

Deterrence/compellence – victim acquiesces to aggressor's demand

Status quo ante – the victim does not change their behavior, may ignore the action, and does not acquiesce.

Defend – victim does not acquiesce and instead builds up defenses in response

Counterattack – victim does not acquiesce and instead attacks the Coercer

[181] The options for the dependent variable are borrowed from the economic coercion and sanctions literature, specifically Daniel Drezner's "The Hidden Hand of Economic Coercion." *International Organization,* 57, Summer 2003, p. 646.

Combination of these responses – victim acquiesces and builds up defenses or victim defends and also launches counterattacks or victim defends and engages in deterrence and compellence against aggressor.

In order to thoroughly examine this question and test the associated hypotheses, this research will consist of an in-depth comparative case study approach. It will assess the strategies of cyber coercion and the cost imposition through the examination of victim responses across two case studies[182]: North Korea's actions against Sony Pictures Entertainment in 2014, and Russian's actions against Estonia in 2007, are well-suited to test the conditions of competing theories and theory building.[183] Further, as noted earlier in this chapter, this research will separately address in-depth the strategies to surmount the purported "attribution problem" that is oft-discussed as a major impediment to examining the actions and outcomes of cyber coercion.

North Korea is a regional power and Estonia is a small power, albeit one that is bolstered by NATO. Russia is a strong power, and Sony Pictures Entertainment is a relatively vulnerable private sector company based in the United States and headquartered in Japan. North Korea's use of cyber capabilities for coercive purposes against Sony Pictures Entertainment and Russian's actions against Estonia each provide a showground to test the focused questions, test the variables that favor successful coercion

[182] Geddes, B. "How the Cases You Choose Affect the Answers You Get: Selection Bias in Comparative Politics." *Political Analysis* 2(1): 1990. p. 131-150.
[183] George, Alexander and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences.* Cambridge: Harvard University Press, 2005.

and for theory building using the lessons resulting from examining these cases. Being able to test these questions and conditions against both a regional power and a strong power aggressor, where the victims of these cases are soft, countervalue targets in a democratic country and a company operating in a democratic country, matters when discussing audience costs. That is, the audience in a democratic country has a greater ability to know what threats might accompany a public use of cyber action than they would under an authoritarian regime. The victim suffers greater audience costs when the media is free to operate, and the victim may incur greater financial losses and pressure on leadership in a free society when a cyberattack occurs and private information is revealed.

The independent variables include the relative responses to George's seven conditions within each case (Clarity of the objective, Strength of Motivation, Asymmetry of Motivation, Sense of Urgency, Adequate Domestic and International Support, Opponent's Fear of Unacceptable Escalation, and Clarity Concerning Precise Terms of the Settlement of a Crisis), and an expanded set of variables that includes financial costs for the victim, audience costs for the victim, leadership destabilization potential for the victim, and targeting of leadership and/or pressure on leadership. These variables are produced by taking the results from the structured focused data drawn from primary and secondary sources. There are caveats to constructing these variables: namely, states and companies have an incentive to withhold this information so as to minimize the public consequences of their victimhood, lessen embarrassment, preserve their dignity and attempt to drive down the overall audience costs. These variables are based on publicly

released information from the victim, publicly available leadership statements, information released from related victims and legal cases, and information based on the commercial cybersecurity industry assessments and its independent access to data. Below is a table showing how each of the independent variables apply to each of the case study dyads:

Table 6:

Independent variables	Russia v. Estonia	North Korea v. Sony
Choice of Target	Countervalue including non-military government	Countervalue
Nature of Attack	Amateur then sophisticated	Sophisticated
Leadership as a target, potential destabilization	Yes, a target No potential destabilization	Yes, a target Yes potential destabilization
Attribution	Yes	Yes
Audience costs for the victim	High	High
Financial costs for the victim	High	High
Pressure on Leadership	Yes	Yes
Clarity of objective	Yes	Yes
Strength of motivation	Yes	Yes
Asymmetry of motivation	No	Yes
Sense of urgency	Yes	Yes
Adequate domestic/international support[184]	Russia: Yes/No Estonia: Yes/Yes	NK: Yes/No Sony: Yes/Unknown
Opponents fear of unacceptable escalation	No	Not at first, but later
Clarity concerning precise terms of the settlement of a crisis	Yes	Yes

[184] In *Forceful Persuasion,* George notes that any successful coercive diplomacy requires a certain level of domestic support and that, a lack of domestic support can constrain the use of coercive diplomacy. Further, he notes that the presence or absence of international support can be important in some cases. p. 78-79

Hypotheses

The hypotheses for this research examining victim response are the following:

Hypothesis 1: George's seven conditions that favor coercive success (Clarity of the objective, Strength of Motivation, Asymmetry of Motivation, Sense of Urgency, Adequate Domestic and International Support, Opponent's Fear of Unacceptable Escalation, and Clarity Concerning Precise Terms of the Settlement of a Crisis) fully explain the outcome without reference to any further factors (i.e. the null hypothesis.)

Hypothesis 2: All other variables being equal, the greater the financial and/or audience costs faced by a victim where there is asymmetric motivation (i.e. one participant in the coercive dyad is more invested in the issue than the other) combined with a potential for leadership destabilization, the more likely the victim is to acquiesce to the demands of the aggressor over time.

Hypothesis 3: If an aggressor chooses solely countervalue, soft or commercial targets that suffer higher audience costs and offer few-to-zero counterattack options, and a fear of escalation, a victim is more likely to acquiesce to stop the pain and ward off future pain.

Research Design

This section outlines how the data for the variables are constructed, what sources are relied upon for the data, how the data will be used to measure what effects the variables (annotated earlier in this chapter) have on the victim responses, and how the cases were selected. The research methodology used in this study will be a qualitative study of mixed research methods focusing on George and Bennett's "structured, focused comparison"[185] between two paired exploratory most-similar case studies to evaluate each case against shared criteria. This allows each the values of the independent variables to be measured consistently.[186] The second method used will be process-tracing as outlined by Bennett and Checkel, Collier, Bennett, Mahoney, Hall and Ricks and Liu.[187]

---

[185] George, Alexander and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences.* Cambridge: Harvard University Press, 2005. Chapter 3, p. 67-72.

[186] The case study research design is guided by the following: George, Alexander and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences.* Cambridge: Harvard University Press, 2005; John Gerring and Lee Cojocaru. "Selecting Cases for Intensive Analysis: A Diversity of Goals and Methods." *Sociological Methods & Research*, 2016, Vol. 45(3) 392-423. John Gerring. *Case Study Research: Principles and Practices (Strategies for Social Inquiry) 2nd Edition*. Cambridge: Cambridge University Press, 2017; David Collier (ed.) "Case Selection, Case Studies, and Causal Inference: A Symposium." *Newsletter of the APSA Organized Section for Qualitative and Mixed-Method Research*, 2008 2:2-16; John Gerring. "What is a Case Study and What is it Good For?" *American Political Science Review*, 2004 98(2): 341-354; and James Mahoney. "After KKV: The New Methodology of Qualitative Research" *World Politics* 62, no. 1 (January 2010): 120-147.

[187] Bennett, Andrew, and Jeffrey T. Checkel. "Process Tracing." *In Process Tracing: From Metaphor to Analytic Tool*, edited by Andrew Bennett and Jeffrey T. Checkel, 3–38. From the Series: Strategies for Social Inquiry. Cambridge: Cambridge University Press, 2014. See also: David Collier, "Understanding Process Tracing." PS: Political Science and Politics , October 2011, Vol. 44, No. 4.
823-830; Andrew Bennett. "Process Tracing and Causal Inference." *Rethinking Social Inquiry: Diverse Tools, Shared Standards,* edited by Henry Brady and David Collier. Plymouth, UK: Rowman & Littlefield Publishers; Second edition, 2010.
Peter Hall "Tracing the Progress of Process-Tracing." *European Political Science*, 2013. 12(1). p 20-30; Jacob Ricks and Amy Liu. "Process-Tracing Research Designs: A Practical Guide." *American Political Science Association*, October 2018. p. 842-846.

This qualitative study is necessary, and a deeper examination of these specific cases is essential, because it is valuable to understand through structured focused questions and process-tracing which factors, how they were operationalized and why they did or did not exert causal influence that led these victims to respond the way they did to cyber coercion. These methods, used in tandem, will serve this purpose by describing in detail the factors that were and were not present in each case study and demonstrating how each factor contributed or did not contribute to the outcome. Further, this research illuminates the mistake of focusing on binary outcomes in a cyber coercive act and shows that examining the degree of effectiveness shown by the victim response *over time* produces a different result and a richer understanding than the simplified, one-moment-in-time might suggest.

The scope of this project is focused on soft, countervalue targets in open, democratic systems. Soft, countervalue targets often incur higher audience costs, affect a larger proportion of society than, say, a counterforce target, and the ramifications for financial loss and leadership pressure can be different from those suffered by counterforce targets. The focus on open, democratic systems is due to better measurement of public pressure and audience costs than is possible or expected in an authoritarian state where public opinion can be manufactured or suppressed.

One limitation of this type of research that is illuminated in the case studies and is pointed out earlier is that aspects of these cyber activities are secretive by nature and therefore insight into these activities can be difficult to observe. Unless the coercer or the victim chooses to disclose the non-public overtures, diplomatic messaging or threats

involved prior to and in the aftermath of a cyber operation, this research must rely on primary sources such as the public statements of officials, the commercial cybersecurity industry notifications of intrusion, the commercial forensic cybersecurity industry assessments and the public statements from victims to collect the data. As well, this research also relies on secondary sources such as news reports and interviews with leaders and critical figures who were involved in the negotiations.

Structured Focused Questions and Process-tracing

To understand how the independent variables shape the victim's decision-making and trace the process over time following a coercive cyberattack, this research will construct data from the case studies via structured focused questions. This method of analysis is structured such that the same questions will be asked of each case study. Chapters four and five present the structured focused comparison comprised of an identical set of questions to illuminate the values for the independent variables, consisting of the seven conditions that favor coercive diplomacy and the extended additional variables.[188] This process allows me to isolate my variables of interest and hold them constant across the cases.

This data will be combined with process-tracing that draws on the chronology sections to understand the in-depth, step-by-step decision making by a victim in the aftermath of a cyber crisis. This data will be used to test the hypotheses on victim

[188] George, Alexander. *Forceful Persuasion*. Washington DC: United States Institute of Peace, 1991. p. 76-81. See also Alexander L. George and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994. p. 279-288.

response to cyber coercion in chapter six. “Process-tracing is an indispensable tool for theory testing and theory development not only because it generates numerous observations within a case, but because these observations must be linked in particular ways to constitute an explanation of the case.”[189] In process-tracing, researchers not only examine their theories of interest, but also must compare and contrast rival theories.[190]

By applying the same structured focused questions to each case, the data revealed can be used to appropriately compare the findings in each case. I will test the hypotheses for this third path, this middle road theory between the two extreme cyber camps, against the identified case studies focused on the North Korea hack of Sony Pictures and Russia's cyberattack against Estonia in 2007 and build a framework within each case to show victim response variation depending on the strategies employed.[191] Process tracing will use the historical evidence from each case to draw conclusions about the causal explanation for that case.[192]

The structured focused questions that will be asked of each dyad are the following:

What were the targets of the cyberattack?

---

[189] George, Alexander and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences.* Cambridge: Harvard University Press, 2005. p. 207.
[190] Hall, Peter. “Tracing the Progress of Process-Tracing.” *European Political Science*, 2013. 12(1). p 20-30. See also: Jacob Ricks and Amy Liu. “Process-Tracing Research Designs: A Practical Guide.” *American Political Science Association*, October 2018. p.842-846.
[191] George, Alexander and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences.* Cambridge: Harvard University Press, 2005. See also David Collier. “Understanding Process Tracing.” *PS: Political Science and Politics* , October 2011, Vol. 44, No. 4 (October 2011), p. 823-830
[192] Bennett, Andrew and Jeffrey Checkel. "Process Tracing: From Philosophical Roots to Best Practices," in Andrew Bennett and Jeffrey Checkel (eds.) *Process Tracing: From Metaphor to Analytic Tool*. Cambridge, Cambridge University Press, 2014.

What was the nature of the attack? How was the attack conducted?

Was leadership targeted?

What was the understanding about attribution at the time of the attack? Did this change over time?

What were the audience costs? What were the audience costs over time?

What were the financial costs? What were the financial costs over time?

What was the pressure on leadership during the cyber crisis?

George's seven conditions as structured focused questions:

What was the victim's understanding of the clarity of the objective?

What was strength of motivation of the coercing power?

What was the asymmetry of motivation between the adversaries?[193]

What was the victim's understanding of the coercer's sense of urgency?

Is there adequate domestic and international support for the victim and the coercer?

What is the opponent's (victim's) fear of unacceptable escalation?

What is the clarity concerning precise terms of the settlement of a crisis for the victim and the coercer?

[193] In *Forceful Persuasion,* George refers to the measurement of asymmetry of motivation as "what is critical in this respect, however, is that the adversary believe that the coercing power is more highly motivated to achieve its crisis objective than the adversary is to prevent it." p. 77.

Case Selection

The research purpose of this project is to examine what effect the variation in coercive strategy, factors present or not present that favor coercive diplomacy have on victim responses to cyber coercive measures over time when the targets are a soft, countervalue targets in open, democratic societies. This research identifies four additional variables beyond George's seven criteria and these two cases are suitable for testing these additional variables and explaining the divergent outcomes. The methodological approach is to study cases in what Gerring and Cojocaru, refer to as 'exploratory most-similar with background conditions similar' positive and negative case studies where there are shared background conditions, but lead to divergent outcomes.[194] The case selection is also informed by Mahoney and Goertz's counsel on small-N qualitative research and the value of including negative cases that are extremely similar to positive cases "to test theory about the causes of outcomes of exceptional interest."[195] Gerring notes,

> "A most similar exploratory design uses cases that "exhibit similar background conditions (Z) and different outcomes (Y). …As always, the research design is more informative if it analyses change through time rather than values at a particular point in time."[196]

---

[194] Gerring, John and Lee Cojocaru. "Selecting Cases for Intensive Analysis: A Diversity of Goals and Methods." *Sociological Methods & Research*, 2016, Vol. 45(3) 392-423. See also, John Gerring. *Case Study Research: Principles and Practices (Strategies for Social Inquiry) 2nd Edition.* Cambridge: Cambridge University Press, 2017. p. 79; and James Mahoney and Gary Goertz. "The Possibility Principle: Choosing Negative Cases in Comparative Research" The American Political Science Review, Nov. 2004, Vol. 98, No. 4, pp. 653-669

[195] Mahoney, James and Gary Goertz. The Possibility Principle: Choosing Negative in Comparative Research. American Political Science Review Vol. 98, No. 4 November 2004. p. 653-669.

[196] Gerring, John. *Case Study Research: Principles and Practices (Strategies for Social Inquiry) 2nd Edition*. Cambridge: Cambridge University Press, 2017.

The purpose of including a positive and negative case is to trace the process on why one victim responds to an aggressors demand with a partial acquiescence response while another victim made a diametrically opposite decision and not only refused to acquiesce but instead heavily defended itself. Beyond that, this victim then coordinated with international institutions and neighboring partners to bolster cyber defenses and resilience for the long-term. Other examples of most-similar negative cases that are part of the population and were considered but excluded from this study include Iran's 2012 attacks against the U.S. financial sector, Iran's 2012 attack against Saudi Arabia's Aramco, and North Korea's 2013 attack against South Korean financial and media outlets. These cases did not share the same background characteristics but are good cases to consider for further research.

The best selection for a most-similar case to the North Korea-Sony cyberattack is the Russia-Estonia case. This research is centered on the North Korea vs. Sony case as the positive case and Russia vs. Estonia as the negative case. These two cases share distinctive, theoretically significant background factors.[197] In both cases, these background vectors include the following:

- In both cases the victims had adversaries who formally declared their demands in public and to governing bodies (For North Korea it was to the United Nations and for Russia its was in the Russian government) in months prior to the conflict;

[197] Gerring, John. *Case Study Research: Principles and Practices (Strategies for Social Inquiry) 2nd Edition*. Cambridge: Cambridge University Press, 2017.

- In both cases they were able to make reasonable attribution in light of the public demand;
- In both cases they were dealing with an aggressor who was extremely committed to the demand;
- In both cases the victim was a democracy or operating in a democracy and therefore more vulnerable to audience costs and financial costs than an authoritarian regime that controls the media and can subsidize losses without oversight;
- In both cases, the victim of the attacks included significant civilian infrastructure that disrupted civilian life for an extended period;
- In both cases the aggressor is a country that is considered "Not Free."[198]

The ranking of "Not Free" also has theoretically relevant underpinnings for this research: namely, these states maintain ubiquitous surveillance over their own populations internally, to include the internet, which contributes to the idea that if cyber coercive acts were originating in their country, they have means to not only be aware of it, but also to control it. With regard to the externalities of being a "Not Free" state, in the realm of cyber coercion, this also means that these states buck the international norms of civil liberties, political pluralism, freedom of expression, openness and transparency, and may be less receptive to following international norms of behavior against pursuing

[198] "Russia." Freedom House, 2007. Located at: https://freedomhouse.org/report/freedom-world/2007/russia and accessed on December 18, 2019. See also "North Korea" Located at: https://freedomhouse.org/country/north-korea/freedom-world/2017 and accessed on December 18, 2019.

civilian targets.

The case selection was also based on two additional factors: first, this research sought dyads where the victims were democratic countries or located within democratic countries because these victims are beholden to variables like audience costs and financial costs in a way that authoritarian regimes are not. The regime type matters because in a democracy there is more oversight to take on higher exogenous costs than there would be in an authoritarian economy where the government will subsidize the financial loss with no transparency to the populace. Further, democratic regimes are more forthcoming with credible information since they must answer to their general public. When dealing with the cyber realm that is already shrouded in secrecy, gaining insight into cyber actions in non-democratic countries, where the leaders are not obligated to the populace and credible information surrounding these actions is highly unlikely to be published due to authoritarian media control, is extremely difficult and the information published often lacks reliability. In order to have best access to transparent, accurate information, including government statements, documents and interviews, examining cases with democratic victims provides greater assurance of the preciseness of the data which is necessary for accurate process tracing. Therefore, democratic victims were specifically part of the case selection process because the level of detailed information that is required for accurate process-tracing would not be available nor be able to be relied upon in a non-democratic or authoritarian regime victim.

The other main factor for case selection were victims that rely significantly upon their IT infrastructure in order to conduct daily functions. Comparing cases where

upwards of 80% of the target population engages with and is reliant upon the digital world daily with a victim where engagement is less than 40% would not be as robust a study because the victim would have ample alternatives to conduct daily life and would not be as drastically affected by variables like audience costs or domestic support. Therefore, I sought cases where the IT usage of the victim was high overall and on par with one another.

Numbers versus Words[199]

Generally, selecting cases based on the dependent variable is a major pitfall in research and doing so carries a dire warning to avoid it. As Achen and Snidal caution, selecting cases based on the dependent variable commits "inferential felonies" that can significantly undermine the validity of one's findings.[200] However, they also concur that "[t]here is nothing wrong with nonrandom samples so long as they are not treated as random. Indeed, there may be good reasons not to choose cases randomly."[201] King, Keohane and Verba's seminal text insisted that qualitative studies ought to avoid selecting cases based on the dependent variable so as not to bias the findings.[202] However, this advice is largely criticized by qualitative methodologists as pertaining more to quantitative and statistical research than to qualitative research.[203] As described below, Mahoney and Collier caution that this advice applies to large-N quantitative studies and not necessarily to qualitative causal models under investigation.[204]

Supporting this view, Gerring highlights "[w]hen the goal is exploratory, it is difficult to envision a viable case-selection strategy that takes no notice of the values for

---

[199] This wording is borrowed from Gary Goertz and James Mahoney's *Tale of Two Cultures: Qualitative and Quantitative Research in the Social Sciences*. Princeton, Princeton University Press, 2012. p. 19.
[200] Achen, H. and Duncan Snidal. "Rational Deterrence Theory and Comparative Case Studies." *World Politics* Vol. 41, No. 2 (Jan., 1989), pp. 143-169. p. 160
[201] Ibid. p. 162
[202] King, Gary, Robert Keohane and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research.* Princeton: Princeton University Press, 1994.
[203] Collier, David and James Mahoney. "Insights and Pitfalls: Selection Bias in Qualitative Research." *World Politics*, Vol. 49, No. 1, October 1996
[204] Ibid.

the outcome of interest.[205] When engaging in causal process tracing, it requires variation on the dependent variable, so it is essential that one must take this need for variation into account when selecting cases. This study seeks to identify a new hypothesis, and by extension a theory, and is considered exploratory.[206] As Gerring notes:

> "Exploratory case selection strategies that select cases based on their outcome, Y, violate a well-worn piece social science folk wisdom not to select based on the dependent variable. This is indeed problematic if a number of cases are chosen, all of which lie on one end of a variables spectrum (they are all positive *or* negative), and the researchers subjects this sample to cross case analysis as if it were representative of a population. …However, this is not the proper or usual employment of cases chosen in an exploratory fashion. First of all, when cases are selected based on the outcome it is usually change in the outcome that is of primary interest."[207]

Similar to George's caveat about creating *conditional* generalizations and not seeking to construct comprehensive generalizations on why coercive diplomacy sometimes succeeds or fails,[208] this research on cyber coercion seeks to do the same but examines an expanded set of variables and provides a strategy to surmount the attribution issue that is specific to cyber coercion and often prevents researchers from pursuing this line of interrogation. If this research sought to create an unencumbered widely generalizable theory about cyber coercion, or was heavily reliant on quantitative data, or

---

[205] Gerring, John. *Case Study Research: Principles and Practices (Strategies for Social Inquiry) 2nd Edition*. Cambridge: Cambridge University Press, 2017. p. 67.
[206] Ibid. p. 65.
[207] Ibid. p. 65.
[208] George, Alexander L. and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994. p. 268.

used a different methodology, then there may be a concern about selection bias.

As Mahoney and Goertz explain, when the objective is to generalize about causal effects for large populations and approach it from a statistical perspective, the standard that all cases ought to be weighted equally absolutely applies.[209] However, if the goal is to examine the constellation of factors on specific cases that lead to particular outcomes, and *why* and *how* they lead to those outcomes, then selecting particular cases is necessary. "Hence, the qualitative concern with substantively important cases seems puzzling from the perspective of the quantitative culture."[210]

Mahoney[211] further expounds on this idea with the following:

> qualitative researchers would never use random selection even among cases from a useful cell…. Instead, they will often select cases about which they have excellent knowledge or can readily obtain such knowledge. In this culture, knowing a great deal about a case contributes significantly to within-case analysis …and can improve one's chances of carrying out valid inference[212]

If this were a different type of study, such as a large-N quantitative study, selection bias would be a major concern because it could invalidate the quality of the results.[213] However, given the exploratory objective of this research and the specific

---

[209] Goertz, Gary and James Mahoney's *Tale of Two Cultures: Qualitative and Quantitative Research in the Social Sciences*. Princeton, Princeton University Press, 2012. p. 171
[210] Ibid. p. 171
[211] James Mahoney previously ran the summer program called the Institute for Qualitative and Multi-Method Research (IQMR) at the Consortium on Qualitative Research Methods at Syracuse University and is a leading academic in social science methodology.
[212] Goertz, Gary and James Mahoney's *Tale of Two Cultures: Qualitative and Quantitative Research in the Social Sciences*. Princeton, Princeton University Press, 2012. p. 19. p 170
[213] Collier, David and James Mahoney. "Insights and Pitfalls: Selection Bias in Qualitative Research." *World Politics*, Vol. 49, No. 1, October 1996

methodology used, it is essential that the value of the outcome be considered during case selection. More specifically, in selecting a positive and a negative most-similar case from the population of cases available, it is inherent to include the outcome in the selection criteria. Further, in conducting causal process-tracing there needs to be variance on the dependent variable and this method of case selection is an acceptable and recommended practice according to Gerring, Mahoney and Collier.

Conclusion

This interdisciplinary study will make an original contribution to the literature in two ways: first, by providing a framework to show under what conditions the cyber realm can be employed for in the coercion dynamic to yield certain victim responses in cyber coercive diplomacy and, second, by providing case studies to test and analyze the proposed framework.

Explaining how victims choose to respond to state-driven cyber coercion over time requires a reevaluation of how we understand aggressive actions in cyber statecraft, and how to apply George's seven conditions that favor coercive diplomacy in the cyber realm. The two camps of cyber conventional wisdom say either cyber actions are trivial and have little effect on the international system (the optimists) or that they will result in cyber-driven disaster and destruction (the pessimists). This research suggests that motivation of both aggressor and victim and whether this is equal or asymmetric as well as financial and/or audience costs shape the victim responses to cyber statecraft actions. Further, that these victim responses are neither the extremes of trivial nor disastrous but are part of the modern international relations landscape and the evolving toolbox for states to exercise their various levers of power.

CHAPTER 3: BACKGROUND AND ORIGINS OF THE INTERNET

The internet is an integral part of life in modern society so how is it possible that it continues to be so vulnerable to cyberattacks? What makes the internet – and therefore a victim – susceptible to these different kinds of cyberattacks and can it be fortified? To thoroughly understand cyber coercion you must first understand the terrain that allows cyberattacks to occur.

In international relations, terrain can be a significant factor for analysis; in the *Tragedy of Great Power Politics,* Mearsheimer discusses the stopping power of water and how large bodies of water inhibit the power projection of military power and the consequences this has on global hegemony.[214] For theory building, it is important to thoroughly understand the constraints and intricacies of the environment in which a theory is operationalized. Is there an equivalent feature in cyberspace to Mearsheimer's theory about the limitations presented by large bodies of water?

In short, no, but it more interesting to understand why not. One could argue that closed systems could come close to Mearsheimer's idea of a cyberspace feature that limits adversarial power projection, but when looking at the open, public internet, there is no equivalent feature. So, what is the terrain and why can it not be secured for soft and

---

[214] Mearsheimer, John. *The Tragedy of Great Power Politics*. W. W. Norton & Company, 2001. Another scholar who examines historical hostilities within a particular terrain is Robert Pape in *Bombing to Win: Air Power and Coercion in War* as well as in "The True Worth of Air Power." *Foreign Affairs*, Issue 2 - March/April 2004, 116-130. Pape provides historical analyses of how conducting hostility via air power can lead to success or failure, depending on the chosen strategy.

hard targets alike? Part of difficulty is based on how the internet grew up.

We have an internet today that was not built with the idea of a trusted digital infrastructure in mind and updating it is not a simple task; it a system of systems. Part of the modern problem of cyberattacks is that society has built our daily lives, our economies, our critical technologies and our crucial services on a system that was not designed nor constructed for the level of connectivity and reliance that we use it for today. The original internet was created by a small group of people whose moonshot goal was to openly share information across the world in near real-time; security, especially as we know it in present day, was not a concern for this massive undertaking at the time. However, now, this "interdependence has created great opportunities and great vulnerabilities, which strategists do not yet fully comprehend.[215]

Where It All Began

Internetworking, or "internet" as it is more commonly known, is simply the practice of connecting multiple computer networks.[216] In May 1961, a graduate student named Leonard Kleinrock at the Massachusetts Institute of Technology wrote a dissertation proposal called "Information Flow in Large Communication Nets"[217] and,

---

[215] Nye Jr., Joseph. ""Nuclear Lessons for Cybersecurity?" *Strategic Studies Quarterly*, Winter 2011. p. 18.
[216] "Protecting the Cybersecurity of America's Networks." *The Brookings Institution*. February 11, 2021. Located at: https://www.brookings.edu/blog/techtank/2021/02/11/protecting-the-cybersecurity-of-americas-networks/
[217]The archived dissertation proposal can be found at: https://www.lk.cs.ucla.edu/data/files/Kleinrock/Information%20Flow%20in%20Large%20Communication%20Nets.pdf

with a small group of fellow academic researchers, would change how people communicate all over the world; Leonard Kleinrock would later be considered the father of Modern Data Networking.[218]

In the proposal, his research focus included "…the nets under consideration consist of nodes, connected to each other by links. The nodes receive, sort, store, and transmit messages that enter and leave via the links… " and he followed this proposal with a July 1961 paper theorizing about how packet switching technology would operate[219] which forms the basic structure of the modern-day internet.

In 1962, two researchers, J. C. R. Licklider and Welden E. Clark wrote a paper following the Spring Joint Computer Conference titled "On-Line Man-Computer Communication"[220] that envisioned using networked computers to exchange data and access programs, identified critical research areas necessary to improve human-computer interactions and laid out four major long-term problems, namely:

> The first of these areas is computer appreciation of natural written languages, in their semantic and pragmatic as well as in their syntactic aspects. The second is computer recognition of words spoken in context by various and unselected talkers. The third is the theory of algorithms, particularly their discovery and simplification. The fourth is heuristic programming. We believe that these four areas will in the long term be extremely important to man computer symbiosis, but that man-computer partnerships of considerable effectiveness and value can

---

[218] Cohen-Almagor, Raphael. "Internet History." *International Journal of Technoethics*, 2(2), 45-64, April-June 2011. p. 47.

[219] The archived theory paper can be found at: https://www.lk.cs.ucla.edu/data/files/Kleinrock/Information%20Flow%20in%20Large%20Communication%20Nets0.pdf

[220] Licklider, JCR and Welden Clark. "On-line Man-Computer Communication. *Proceedings of the Spring Joint Computer Conference.* Archived at the Internet Archive and located at: https://archive.org/details/online-man-computer-communication/page/n3/mode/2up

> be achieved without them. We suspect that solutions in these areas will be found with the aid of early man-computer symbioses, rather than conversely.[221]

Aspects of the four problems that Licklider and Clark identified 58 years ago continue to be worked on, updated and improved upon today. We have successfully created computer appreciation of natural written languages, but it continues to develop. Siri, Alexa, the suite of digital personal assistants and various accessibility tools that recognize voice have satisfied the second major problem of computer recognition of words spoken at a basic level, but that, too, continues to develop. The third and fourth long-term problems, computer algorithms and heuristic programming, continue to be areas of great discovery and expansion.

This research formed the basis for a U.S. Department of Defense-funded project, begun in 1962 and headed by Licklider, at the Advanced Research Project Agency (ARPA)[222] that would eventually grow to be called the Advanced Research Projects Agency Network, or ARPANET. ARPANET was one of several Cold War projects that were part of a series of innovative technological research projects initiated in the aftermath of the Soviet Union's successful Sputnik satellite launch. ARPANET grew slowly; in 1965 the proof of concept was successfully tested via a low-speed dial-up

---

[221] Licklider, JCR and Welden Clark. "On-line Man-Computer Communication. Archived at the Internet Archive and located at: https://archive.org/details/online-man-computer-communication/page/n3/mode/2up. Page 122. Licklider and Clark's paper includes a prescient statement, especially when writing in 1962: "Twenty years from now, some form of keyboard operation will doubtless be taught in kindergarten, and forty years from now keyboards may be as universal as pencils, but at present good typists are few. Some other symbolic input channel than the typewriter is greatly needed." page 115.

[222] Over the years the agency has changed its name four times from Advanced Research Projects Agency (ARPA) to the Defense Advanced Research Projects Agency (DARPA) and back again. The current name in 2021 is the Defense Advanced Research Projects Agency (DARPA).

telephone line[223] that connected a computer in Massachusetts with one in California.[224]

By 1969, ARPANET was officially launched, connecting four computer nodes in the first long-haul network that included the University of California at Los Angeles (UCLA), the Stanford Research Institute (SRI) in Menlo Park, California, the University of California at Santa Barbara (UCSB), and the University of Utah. In the next decade, ARPANET would expand dramatically; it consisted of 35 nodes by 1973, and in 1974 a set of new protocols called Transmission Control Protocol (TCP) and the Internet Protocol (IP) were implemented.[225] These protocols govern how a network establishes and breaks connections, organizes and routes data packets, and checks for errors. The TCP/IP protocol is still widely in use today, a testament to the open architecture implementation, although several other protocols have also been developed in the intervening 46 years. The following diagrams[226] show the growth of ARPANET from initial 4-node network success to significant growth by 1977:

---

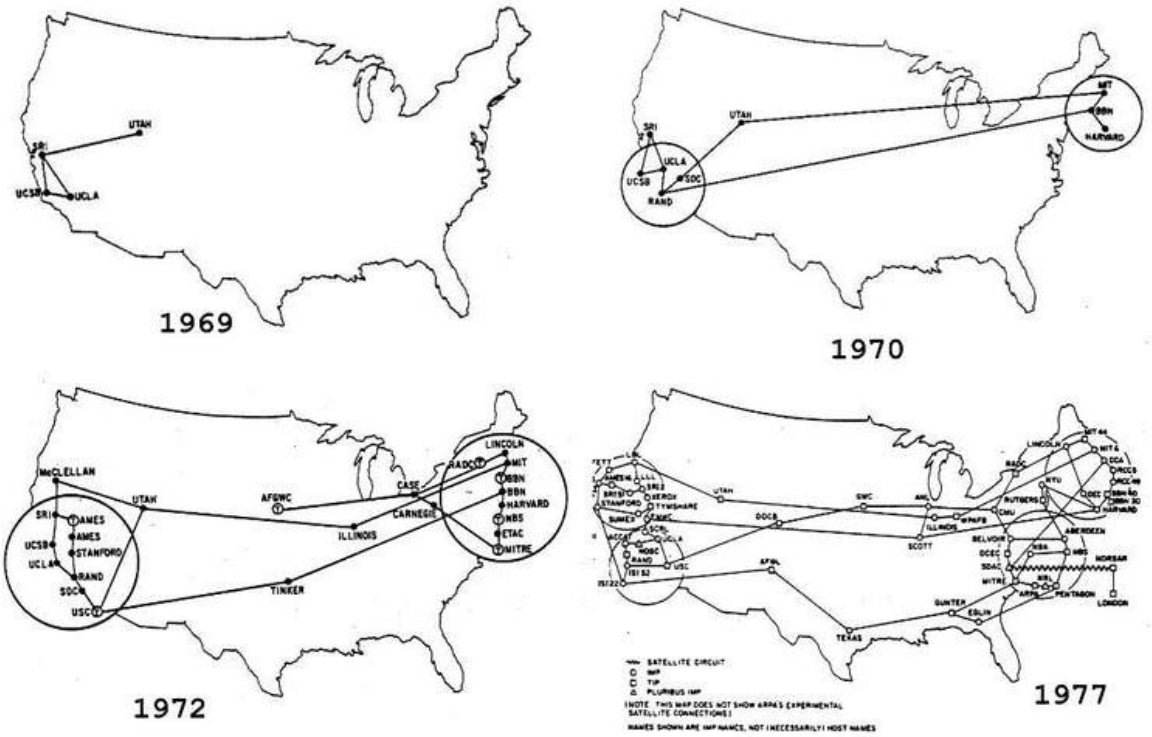
[223] To put the magnitude of this endeavor in context, it was only 62 years earlier that the first radio transmission from the United States crossed the Atlantic Ocean. The first U.S. radio transmission across the Atlantic Ocean came from Marconi Station on Cape Cod to England. The message was from President Theodore Roosevelt to King Edward VII in London, praised wireless telegraphy and greeted the monarch.
https://www.edn.com/marconi-sends-transatlantic-wireless-message-january-19-1903/

[224] "The History of the Internet" via The Department of Computer Science Old Dominion University. Located at: https://www.cs.odu.edu/~tkennedy/cs300/development/Public/M02-HistoryOftheInternet/index.html#:~:text=1965%3A%20Working%20with%20Thomas%20Merrill,area%20computer%20network%20ever%20built. Accessed February 1, 2021.

[225] Cohen-Almagor, Raphael. "Internet History." *International Journal of Technoethics*, 2(2), 45-64, April-June 2011. p. 50.

[226] Shultz, Colin. "See How Fast ARPANET Spread in Just Eight Years." *Smithsonian Magazine*. August 28, 2013. Located at: https://www.smithsonianmag.com/smart-news/see-how-fast-arpanet-spread-in-just-eight-years-2341268/ and accessed on February 1, 2021.

Figure 3:



It took 15 years to grow from MIT graduate student Leonard Kleinrock's idea and theoretical conception to a government-funded innovation project with rapid expansion to eventually become a fully-fledged operational system of networked computers with transatlantic connectivity. This would continue to grow, innovate and improve in the 1980s, and by "January 1983, enough individual networks had networked with each other that the ARPANET had evolved into the internet, although the original ARPANET itself was not formally decommissioned until 1990."[227] With the expansion of the internet, came fear and doubt. Fear that all of our critical and financial systems would come

[227] "ARPANET." Defense Advanced Research Project Agency. Located at: https://www.darpa.mil/attachments/ARPANET_final.pdf. Accessed February 2, 2020.

crashing down in the Y2K fiasco that was New Year's Eve 2000. And doubt that the internet would ever be more than a "passing fad" and that this new-fangled technology was not going to significantly impact our daily lives, as the December 5, 2000, *Daily Mail* noted:

Figure 4:

Daily Mail, Tuesday, December 5, 2000 Page 33

Internet 'may be just a passing fad as millions give up on it'

THE Internet may be only a passing fad for many users, according to a report.

Researchers found that millions were turning their back on the world wide web, frustrated by its limitations and unwilling to pay high access charges.

They say that e-mail, far from replacing other forms of communication, is adding to an overload of information.

Experts from the Virtual Society project, which published the report, say predictions that the Internet would revolutionise the way society works have proved wildly inaccurate.

Many teenagers are using the Internet less now than previously, they conclude, and the future of online shopping is limited. Steve

By James Chapman
Science Correspondent

Woolgar, director of the society, said: "We are often presented with a picture of burgeoning Internet use, but there is evidence already of drop-off and saturation among users.

"Teenagers' use of the Internet has declined. They were energised by what you can do on the Net but they have been through all that and then realised there is more to life in the real world and gone back to it."

The project, sponsored by the Economic and Social Research Council, gathered together research by 25 universities across Europe and the U.S.

It estimated that in Britain alone there could be more than two million people who regularly used the Internet but had now given up.

Analysts say some simply became bored, while others were frustrated by the amount of

Net loss: Two million Britons have logged off the Internet

Although this popular publication quipped that people may give up on the internet 21 years ago, that did not happen. According to the International Telecommunications Union (ITU), the primary source for global radio and telecommunications connectivity information and the United Nations agency for information and communication technologies (ICTs), about 4 billion people or more than 51% of the global population is

using the internet as of 2019.[228] Industry leader, Cisco, estimates that nearly two-thirds of the world's population will have internet access by 2023, totaling 5.3 billion users.[229] That number refers to overall users, not devices. Cisco estimates that by 2023 the number of connected devices will be three times the total global population. "There will be 3.6 networked devices per capita by 2023, up from 2.4 networked devices per capita in 2018. There will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018."[230] Each device represents a potential cyberattack vector for an aggressor and a vulnerability for a user.

The distribution of internet users, however, is uneven as shown in this map from Pew Research[231] and this table from Cisco:[232]

[228] International Telecommunications Union, Statistics. Located at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Accessed on February 2, 2021.
[229] Cisco Annual Internet Report (2018-2023) White Paper. March 9, 2020. Located at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed January 8. 2021.
[230] Ibid.
[231] Pew Research, https://www.pewresearch.org/fact-tank/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/
[232] Cisco Annual Internet Report (2018-2023) White Paper. March 9, 2020. Located at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed January 8. 2021.

Figure 5. Internet Use Across the World

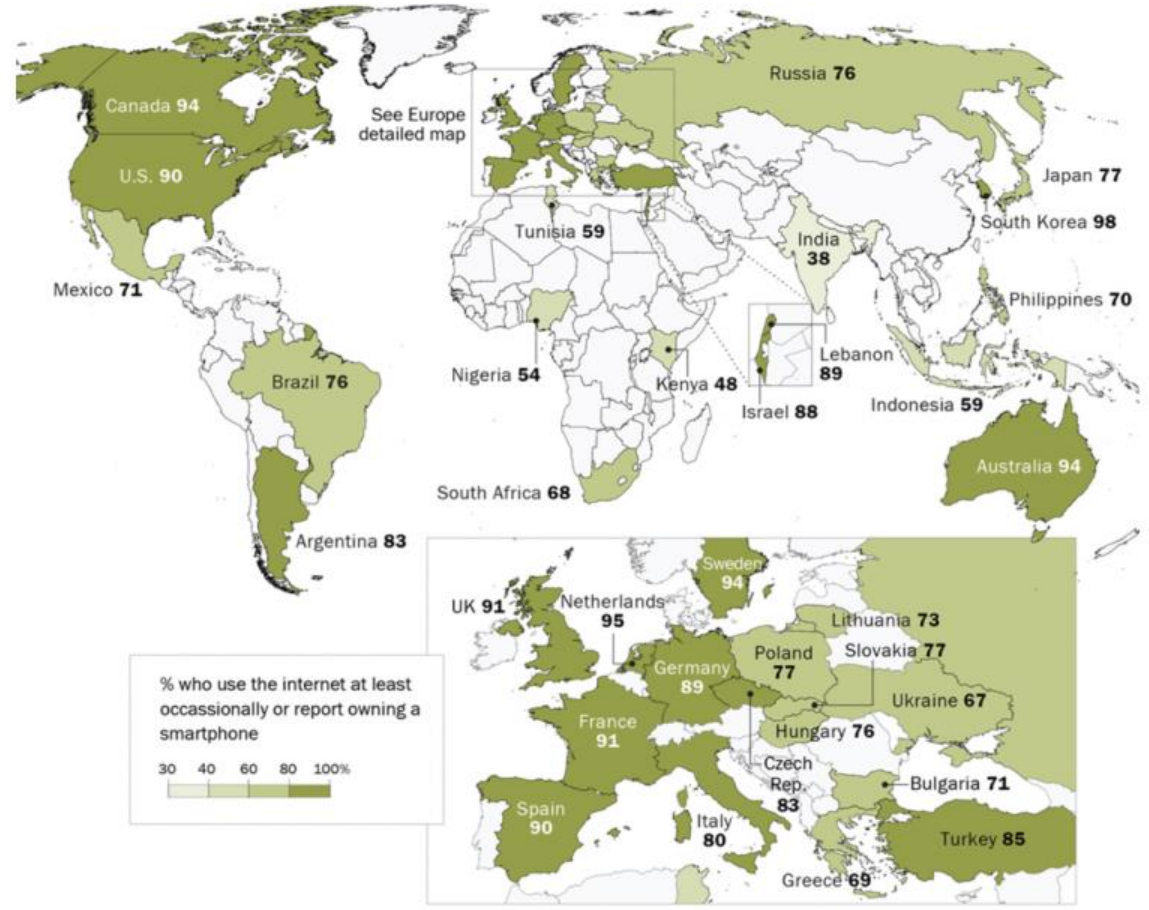


Figure 6. Internet users as a percentage of regional population

Region	2018	2023
Global	51%	66%
Asia Pacific	52%	72%
Central and Eastern Europe	65%	78%
Latin America	60%	70%
Middle East and Africa	24%	35%
North America	90%	92%
Western Europe	82%	87%

The lop-sided distribution of internet users means that countries and entities that are more reliant on the internet for its critical services may also be more vulnerable to potential cyberattacks and activities like cyber coercion.

In addition to the physical connectivity that the internet provides, modern day internet consists of networked devices, so the other significant component to understanding the landscape of contemporary cyberspace is Moore's Law. Originally, Moore's law is the observation that the number of transistors in a dense integrated circuit (the chip speed) doubles every two years, and the cost is halved during this same timeframe. It is an economic argument as well as a technological one; faster chips allow

faster processing, increased complexity and capacity, advanced processes, and increased performance. A contemporary interpretation is a focus on the increase of cores per die instead of simply clock speed, as was the original Moore's law. A core is a unit that runs in parallel with other cores and a die consists of several cores.

Considerations of Moore's law matters when analyzing offensive and defensive operations and capabilities in cyberspace, especially when comparing operations differentiated in time by more than two to four years. The difference between what was possible in cyberspace in 2002 compared with 2006, or 2010 compared with 2016, or more drastically, what was possible in 2002 versus what is possible in 2020 is massive. It is no longer a one-to-one comparison when analyzing capabilities across an 18-year time span due, in part, to the effect of Moore's law. This is a contributing factor to why it is difficult to do long range longitudinal study on cyberspace operations unless explicitly accounting for the technical differences as a factor in the final analysis, which several scholars fail to factor in. If a scholarly argument is based upon an assumption about a technological capability at the time, it may not have great explanatory value in the future due to the constantly innovating environment and increase in speed and capability that Moore's law demonstrates.

For example, when writing in Winter 2016/2017, Slayton highlights that the Chinese firewall is not as impervious as one may think and can be "easily circumvented,"[233] citing studies that use data from 2006, 2007 and 2010.[234] While that

[233] Slayton, Rebecca. "What is the Cyber Offense-Defense Balance?" *International Security* 41:3. Winter 2016/2017. p. 75.
[234] This reference from Slayton's paper is a paper that was eventually published in 2007 and

may have been true during the time frame of the original study, it ill-advised to assume that is still the case in 2016, given the significant generational improvement in technology in the intervening years between 2010 and when she is writing, let alone with the present day 2021.[235] This is simply one example where the explanatory value of an argument loses power because it is based on data that is, conservatively, at least five generations old, technologically speaking.

This disconnect exemplifies one aspect of the challenge when writing about the intersection of cyberspace and international relations. Since technological capabilities significantly improve (i.e. Moore's law) in a relatively short timeframe (e.g. two years) it can be difficult to look across studies from even the last decade and draw accurate conclusions about the present-day state of cyber capabilities. For example, when conducting operations in cyberspace, speed of execution can make the critical difference between success and failure; the difference between being victorious and being caught. The speed of execution can also have several dependencies including the connectivity speed of the network, hardware speed of the devices in the network, efficiency of the code written to run the commands, and the complexity of the network. If an adversary is able to gain access to a network undetected and is able to navigate through the network

---

relied on data from 2006 and earlier on China's technology for packet inspection on traffic: Richard Clayton, Steven J. Murdoch, and Robert N.M. Watson, "Ignoring the Great Firewall of China," paper presented at the Sixth Workshop on Privacy Enhancing Technologies, Robinson College, Cambridge, United Kingdom, June 28–30, 2006. The second reference from Slayton relied on data from 2007 and 2010 in a work by David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue*, Vol. 44, No. 2, April 2013, p. 147–164.

[235] For a thorough discussion of the Great Firewall of China in recent years, see James Griffiths. *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. London: Zed Books, 2019.

unnoticed (e.g. if a potential victim does not have adequate cybersecurity practices, poor cyber hygiene, a lack of critical controls, lack of monitoring, etc.) then the importance of the need for speed disappears.[236] This is the likely scenario for the hack of Sony Pictures Entertainment; it appears from the amount of the data stolen and the extent to which the network was wiped that the hackers had the luxury of time to navigate through the network, gather extensive data, and leave behind malware that destroyed the hardware.

[236] For a complete accounting of the recommended critical controls that SPE lacked at the time, see Gabriel Sanchez. "Case Study: Critical Controls that Sony Should Have Implemented." *SANS White Paper*, June 1, 2015.

CHAPTER 4: SONY PICTURES ENTERTAINMENT CASE STUDY

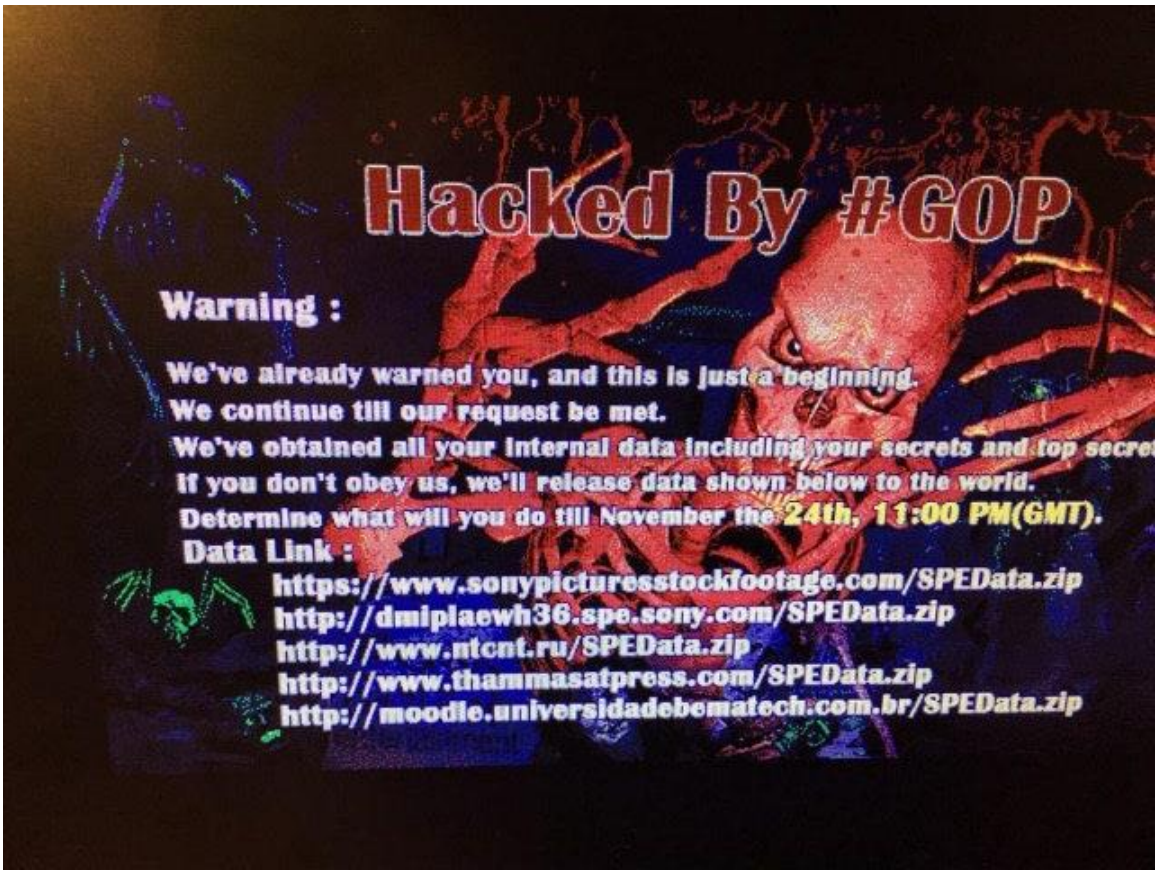


Figure 7: A photo of a screen showing what is apparently the skull splash page that appeared on Sony company computers when the attack started, posted by someone who said he was a former Sony employee who was sent the image by current Sony employees. The image was first posted on Reddit.[237]

The conventional wisdom on the case study of North Korea's actions against Sony Pictures Entertainment is that the cyber coercion was a failure because the movie was eventually released. As one scholar, writing about deterrence failures in cyberspace

[237] Zetter, Kim. "Sony Got Hacked Hard: What We Know and Don't Know So Far." *Wired*, December 3, 2014. Located at: https://www.wired.com/2014/12/sony-hack-what-we-know/ and accessed December 2, 2019.

noted, "and millions of Americans watched *The Interview*"[238] implying that the fact that some Americans watched the movie means that the North Korean effort was a failure. As another scholar remarked:

> "…an obvious [example] of an attempted coercion effort in cyberspace that did not succeed is the North Korean effort to stop the release of *The Interview* by attacking Sony. When you walk through the coercion theory as commonly understood, every single advantage was on the North Korean side there and you would expect that course of activity to work… and… I mean, it didn't. *The Interview* became this preposterous movie that somehow turned into a cause for freedom of speech online – rent it online and do your part for American freedom of speech.[239]

When examined in detail over an expanded timeframe, it was not a failure; it may not have fully achieved its original goal of the victim completely cancelling the film, but North Korea's actions caused Sony Pictures to take several, costly steps and limit release of the film, due in part to a number of factors including audience costs, over time. Sony Pictures changed its behavior due to the cyber coercion. The release date was first cancelled and then the release plans modified, promotion of the film was cancelled, the market share for the eventual film release was heavily pared down resulting in financial losses, and another film called "Pyongyang" from Fox was cancelled[240] due to the fear of additional cyberattacks. A foreign government was effectively demanding censorship of

---

[238] Lindsay, Jon. "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack." Journal of Cybersecurity, 1(1), 2015, 62.
[239] Evans, Ryan. "Is Cyber Half the Battle?" *War on the Rocks interview with Ben Buchanan, Erica Borghard and Fiona Cunningham*, podcast audio, May 12, 2020. https://warontherocks.com/2020/05/is-cyber-half-the-battle
[240] "Sony Cancels 'Interview' Release After Theatres Drop Out While Fox Folds Similar Movie." *NBC News*, December 17, 2014. Accessed via https://www.nbcnews.com/storyline/sony-hack/sony-cancels-interview-release-after-theaters-drop-out-while-fox-n270281 on April 2, 2018.

a multinational corporation located in the United States, and being successful, at least partially, to get the company to change its behavior, as measured over three different temporal values. North Korea's actions and the subsequent audience costs resulted in a Sony Executive losing their job, North Korea embarrassed important business associates of Sony Pictures when they publicly released damaging and humiliating emails, and Sony suffered significant financial losses all while getting a reduced viewership of the film North Korea wanted shut down.[241] Tracing the process and parsing out the details of the cyber operation against Sony Pictures Entertainment will show the additional factors involved in creating successful cyber coercion and forcing the victim to change its behavior.

Background

In 2014, Sony Pictures Entertainment (SPE) produced a satirical comedy called "The Interview" starring Seth Rogen and James Franco playing a talk show host and his producer hired to kill North Korean leader Kim Jong-un. It was a farce comedy, but North Korea perceived it as an affront. In response, the cyberattack campaign against Sony Pictures Entertainment was a multi-stage strategy, not a hasty action, which is evident once the components, specific actions and timeline of the hack are examined. This was not a simple cybercrime to pilfer funds; this cyberattack had a purpose: to halt

[241] Hess, Amanda. "Inside the Sony Hack." *Slate,* November 22, 2015. Accessed via http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html on March 28, 2018. See also "Company-Wide Consequences of Sony's Data Breach" *Promisec Report, 2017.*

distribution of "The Interview," to punish Sony Pictures Entertainment for its production, and to leave lasting damage to its networks and systems. The particular cyber capabilities used, how they were used, the timing of the stages of the cyberattack and the actions taken by the aggressor reveal the coercive strategy. The attackers penetrated Sony Pictures Entertainment networks, stole vast quantities of data, destroyed the computers and servers and then engaged in a deliberate, multi-phase leak to increase pressure on the company.

Sony Pictures Entertainment was alerted to the attack on November 24, 2014, but the attackers likely had been inside Sony Pictures Entertainment systems for months. The culprits claimed to be a group called "Guardians of Peace" or "GOP" but in reality, it was a group known to the cybersecurity world as Lazarus, which is attributed to North Korea.[242] This group stole large amounts of data, including unreleased films, internal emails, and the personally identifying information of about 47,000 employees and actors.[243] They then proceeded to leak sensitive, internal documents from Sony Pictures Entertainment in the ensuing weeks in an effort to ratchet up the pressure on Sony Pictures Entertainment.

It worked, at first, but Sony Pictures Entertainment eventually decided it would not fully comply with the coercion demand and proceeded with a limited video release.

---

[242] Tsing, William. "The Advanced Persistent Threat files: Lazarus Group." *MalwareBytes Labs*, March 12, 2019. Located at: https://blog.malwarebytes.com/threat-analysis/2019/03/the-advanced-persistent-threat-files-lazarus-group/ and accessed on January 15, 2021.
[243] Fritz, Ben and Danny Yadron. "Sony Hack Exposed Personal Data of Hollywood Stars; Breach Includes Social Security Numbers for 47,000 Employees and Actors, Including Sylvester Stallone, Judd Apatow and Rebel Wilson. *The Wall Street Journal*, December 5, 2014.

This limited video release was significantly scaled down from the planned December holiday release. Sony Pictures Entertainment changed its behavior due to the cyberattack; it did not fully comply with the demand of the aggressor, but it did partially, it lost money in doing so, a Sony Pictures Entertainment Executive lost their job, and future Sony - Pictures Entertainment and other production company's planned films with North Korean angles were scrapped. North Korea's actions were able to significantly impact the behavior of this multinational company and others in the entertainment industry. The cyberattack resulted in a successful partial compellence from the victim and deterred not only the victim but other potential players from producing films with North Korea-based plotlines.

Backlash of some form was somewhat expected by Sony Pictures, but the extensive method of coercion appears to have been a surprise. Earlier in the year, in June 2014, Sony Pictures President Doug Belgrad sent a note to Sony Entertainment Chief, Michael Lynton, his boss, noting the sensitive nature of depicting the assassination of a living leader and offering his assistance to address the concerns. Soon thereafter, Mr. Lynton approved more than one-half million dollars to digitally scrub images of former North Korean leaders from the movie. By July, executives at Sony in Japan, the parent company, expressed concern and did not want a farcical movie to endanger international relations for Japan and North Korea. In order to distance itself slightly from the movie, it was not promoted on Sony Pictures' website, and it carried the brand Columbia Pictures, a Sony label, but not Sony Pictures.[244] The plan was that the movie was going to be

[244] Fritz, Ben, Erich Schwartzel and Barret Devlin. "Sony Pulls Korea Film "The Interview;" U.S.

released, with some distance between the movie and the company, but nothing overly drastic.

Cyberattack

The cyberattack campaign consisted of completely destroying a significant portion of Sony's computer network, making the recovery of data impossible, rendering the hardware unusable, publishing nine rounds of stolen internal data, suffering additional public threats, and leaving an inability for Sony Pictures Entertainment to use parts of the computer network for weeks to months. The crisis phase lasted 25 days, from November 24, 2014, to December 19, 2014, with months more of network remediation and dealing with the public relations fallout. The attack resulted in causing Sony Pictures Entertainment to lose millions of dollars in number of ways.

The loss included having their information technology systems crippled, some for months and some forever that required new equipment; limiting release of the film; losing revenue from the anticipated sales of the leaked films; and, suffering great public embarrassment in having their catty, mocking internal documents exposed, especially in an industry that trades on flattery and fawning. Due to the nature of the content of the messages, SPE also had to deal with significant, long-term fallout of the humiliation in the business world in which they operate, resulting in the removal of a leader at Sony Pictures Entertainment.

According to the CEO, Michael Lynton, "the bigger challenge was that the folks

---

Blames Pyongyang for Hack; Studio Scraps Dec. 25 Debut After Terrorist Threats Prompted Movie Chains to Skip Film." *The Wall Street Journal*, December 18, 2014.

who did this didn't just steal practically everything from the house; they burned the house down. They took our data. Then they wiped stuff off our computers. And then they destroyed our servers and our computers."[245] In addition to this damage, "four unreleased movies produced by Sony were leaked online to file-sharing websites. The pirated copies of films available online include "Fury," "Still Alice," "Annie," "Mr. Turner" and "To write love on her arms," all of which are due for official release"[246] in December 2014 and in 2015 with one of the films being downloaded 1.2million times in a week. This was a further financial loss for SPE due to lost revenue from the future releases of these films.[247] The CEO noted that he believed the GOP also stole "The Interview," but chose not to release it.[248]

Overall, the cyberattack malware crawled through the network, destroying half of its global computer system. "It erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers."[249] Further, to ensure failure of any recovery efforts, the data was overwritten seven different ways and the startup software, needed to run the initiation of the system, was destroyed thus reducing the machines to a

---

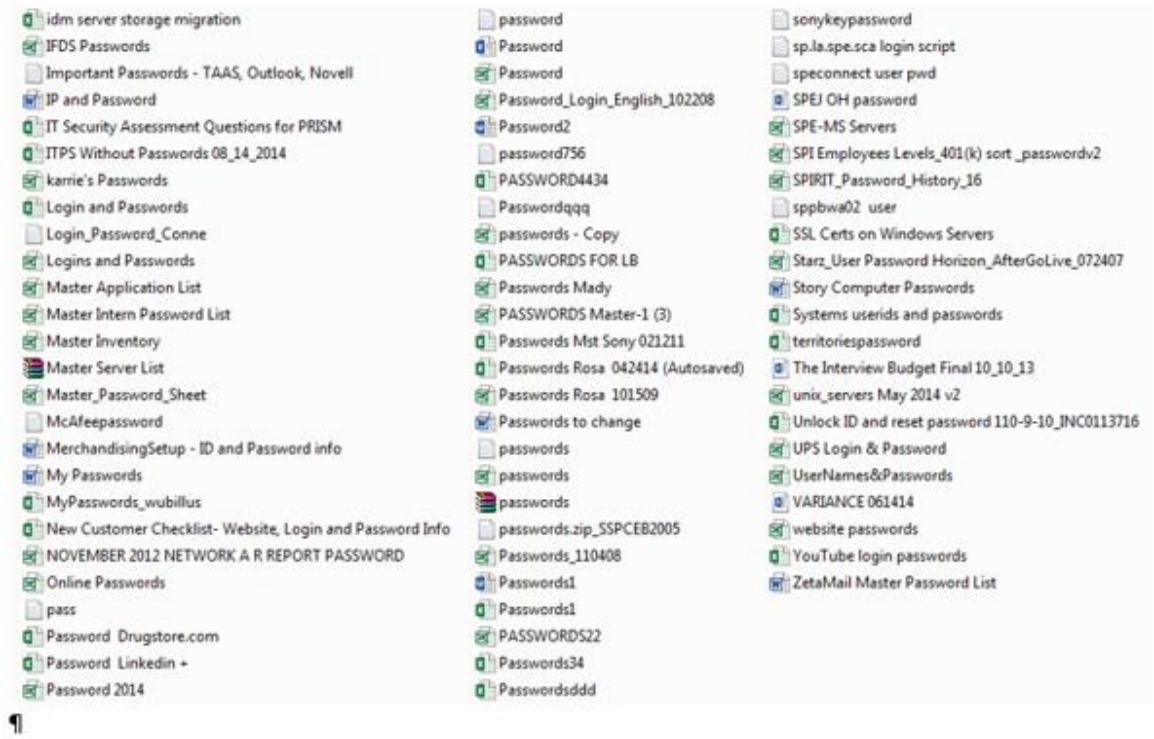
[245] Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review*, July–August 2015.
[246] Osborne, Charlie. "Sony hires FireEye's Mandiant following internal security breach." *ZDNET*, December 1, 2014.
[247] Osborne, Charlie. "Sony hires FireEye's Mandiant following internal security breach." *ZDNET*, December 1, 2014.
[248] Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review*, July–August 2015.
[249] Elkind, Peter. "Inside the Hack of the Century." Fortune Magazine (New York, NY),June 25, 2015. p. 66.

chunk of useless metal.[250] This was a well-planned and smartly executed attack that left the victim with a severely damaged network, an inability to operate in key areas, a huge financial bill for the hardware and remediation, and a multi-phase leak of internal documents that served to ratchet up the pressure on leadership with each subsequent leak.

One example of the type of data stolen and leaked is the following folder list that, likely the hackers, called "Password" and proceeded to dump all files they found on the network that contained passwords. This folder was included in the second round of published files on December 3, 2014 and is shown in Figure 8.[251]

[250] Ibid.
[251] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

Figure 8:



¶

On December 8, 2014, Sony Pictures Entertainment sent a letter to SPE employees calling it a "brazen cyberattack."[252] The letter also warned employees that their personally identifying information (e.g., social security number, medical information, driver's license, etc.) was stolen and provided arrangements with a third-party identity protection company, at Sony's cost, for the employees to contact.

Sony Pictures Entertainment initially did not acquiesce to the demand to withhold the film, especially given that they had already made costly additional digital edits of the film to make it less gory in the summer of 2014 to assuage Sony executives in Japan concerned about increasing tensions with North Korea.[253] When the cyberattack was

[252] Letter to Sony Employees, Sony Pictures Entertainment, December 8, 2014.
[253] Seal, Mark. "An Exclusive Look at Sony's Hacking Saga." *Vanity Fair*, February 4, 2015.

initially discovered, Sony Pictures ignored the demand and focused on the technical problems with the network, managing employee expectations, and keeping the business running using analog options such as fulfilling payroll without a computer system. However, following the subsequent rounds of leaked data, additional threats and refusal from major distributors to air the film, Sony changed course and cancelled the release. That decision was then reversed on December 21, 2014, and changed to a limited release, paring down how and where it would be released, along with releasing it via streaming services, resulting in additional financial losses. SPE decided to release the movie through whatever limited means might be available but also balanced this desire with ensuring that "the rights of its employees and the rights of the movie-going public are going to be protected."[254] Meanwhile, other production outlets cancelled films featuring North Korea in the plot[255] due to the fear of additional cyberattacks and threats.

[254] Lee, Edmund. "You Will Get to See "The Interview," Sony Lawyer Says." *Vox,* December 21, 2014.
[255] "Sony Cancels 'Interview' Release After Theatres Drop Out While Fox Folds Similar Movie." *NBC News,* December 17, 2014. Accessed via https://www.nbcnews.com/storyline/sony-hack/sony-cancels-interview-release-after-theaters-drop-out-while-fox-n270281 on April 2, 2018.

Chronology for Process Tracing

March 2014: The movie, *The Interview*, has the second test screening with studio executives present. The co-producers and directors Seth Rogen and Evan Goldberg, said "The audiences loved the movie, and so the studio was thrilled."[256]

June 2014: Lynton sought and received assurances from a RAND Corporation senior defense analyst, in consultation with the State Department's special envoy for North Korean human rights issues, that the North Korean antagonistic narratives concerning the movie was just rhetoric and "that this is typical North Korean bullying, likely without follow-up, but you never know with North Korea."[257]

June 2014: North Korean state KCNA news agency said, "making and releasing a movie on a plot to hurt our top-level leadership is the most blatant act of terrorism and war and will absolutely not be tolerated."[258] Typical of the DPRK, continued hyperbolic statements came out from its spokespeople, including "'The U.S. has gone reckless in such provocative hysteria as bribing a rogue movie maker to dare hurt the dignity of the supreme leadership of the DPRK," a foreign ministry spokesman said in a statement."[259] According to leaked emails, Kazuo Hirai, the Tokyo-based CEO and President of Sony, the parent company of SPE, was extremely concerned about the film, especially considering the volatile relationship between Japan and North Korea.[260]

June 25, 2014: Seth Rogen replied to the threat by tweeting, "People don't usually wanna kill me for one of my movies until after they've paid 12 bucks for it. Hiyooooo!!!"[261]

July 2014: The North Korean UN Ambassador Ja Song Nam argued against the production and distribution of the film in a letter to the UN Secretary General, stating that "To allow the production and distribution of such a film on the assassination of an incumbent head of a sovereign state should be regarded as the most undisguised sponsoring of terrorism as well as an act of war."[262]

---

[256] Seal, Mark. "An Exclusive Look at Sony's Hacking Saga." *Vanity Fair*, February 4, 2015.
[257] Seal, Mark. "An Exclusive Look at Sony's Hacking Saga." *Vanity Fair*, February 4, 2015.
[258] Bennett, Bruce. "Did North Korea Hack Sony?" *RAND*, December 11, 2014.
[259] Neuman, Scott. "North Korea Threatens War Over New Seth Rogen Comedy." *NPR*, June 25, 2014. See also "DPRK accuses U.S. film of insulting its leadership" *Xinhua*, June 25, 2014.
[260] Seal, Mark. "An Exclusive Look at Sony's Hacking Saga." *Vanity Fair*, February 4, 2015.
[261] Rogen, Seth. June 25, 2014. https://twitter.com/Sethrogen/status/481811214737997825
[262] Beaumont-Thomas, Ben. "North Korea complains to UN about Seth Rogen comedy The Interview." *The Guardian*, July 10, 2014. Located at: https://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco

September 2014: Discussions continued at SPE and with Sony regarding making changes to the film to ease tension with North Korea. Amy Pascal exchanged emails with Kazuo Hirai discussing changed to the final scene. She wrote: "There is no face melting, less fire in the hair, fewer embers on the face, and the head explosion has been considerably obscured by the fire, as well as darkened to look less like flesh."[263]

November 21, 2014: Co-chairmen of Sony Pictures Entertainment, Amy Pascal and Michael Lynton as well as other SPE executives were sent an email from a group called "God'sApstls," demanding compensation and to "pay the damage, or Sony Pictures will be bombarded as a whole."[264] Unfortunately, neither Pascal nor Lynton saw the email, Pascal's going to her spam folder and Lynton's being buried in his inbox.

November 24, 2014: Sony Pictures Entertainment employees arrived to find the "Hacked By #GOP" message on their computer screens framed by red skeletons with the warning: "*We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data shown below to the world."* The data referenced were five links that contained the internal communications of SPE that had been harvested over the weeks prior.[265]

Amy Pascal, the co-chairman of Sony Pictures Entertainment, was greeted by this message on her screen upon arriving at the office and then she phoned SPE CEO Michael Lynton. Lynton advised her that he had been notified by the SPE CFO David Hendler and that they had been hacked. He informed Amy that they would shut down the SPE computer network, including any customer-facing sites, that there was no ability to log on and that the 3500 employees were instructed to shut down their computers, not to e-mail or download anything on the company lot and were sent home.[266] Within hours the fact Sony was hacked was made public.

November 26, 2014: Four torrent links were published that contained unreleased movies from Sony that GOP obtained during the cyberattack. The films included include "Fury," "Still Alice," "Annie," "Mr. Turner" and "To write love on her arms," which planned to be released in December 2014 and in 2015.[267] One of these films was downloaded over 1.2million times in one week.[268]

---

[263] Miller, Daniel. "Future of Sony's Amy Pascal questioned after hacked email revelations." *Los Angeles Times,* December 11, 2014.
[264] Seal, Mark. "An Exclusive Look at Sony's Hacking Saga." *Vanity Fair*, February 4, 2015.
[265] Seal, Mark. "An Exclusive Look at Sony's Hacking Saga." *Vanity Fair*, February 4, 2015.
[266] Seal, Mark. "An Exclusive Look at Sony's Hacking Saga." *Vanity Fair*, February 4, 2015.
[267] Osborne, Charlie. "Sony hires FireEye's Mandiant following internal security breach." *ZDNET,* December 1, 2014.
[268] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

December 1, 2014: Round One Published - the first round of hacked data is published and consists of a full cache of data files totaling 24.87GB of compressed files that contain 33,880 files and 4,864 folders. The data consist of thousands of social security numbers, personal information, human resources information, dates of birth, contact phone numbers, compensation details, retirement plans, termination plans, executive salaries, copies of passports, and other sensitive documentation.[269] Sony Pictures Entertainment hires well-known cybersecurity firm, FireEye, led by Kevin Mandia, to assist.

December 1, 2014: When asked if North Korea was involved with the cyberattack, the spokesman for North Korea's United Nations mission said, "I kindly advise you to wait and see."[270]

December 3, 2014: Round Two Published – the second round of hacked data is published and, although smaller in size, this one consists of the most sensitive data, totaling more than 11,000 files. It includes full security certificate information, authentication credentials and a variety of internal and external account credentials used at Sony Pictures Entertainment to conduct business.[271] The published documents also included everything needed for daily maintenance on the Sony network, including the "files detailing how to access QA, [quality assurance] staging, and production database servers – with a master asset lists that map the location of database (Oracle, Sybase, and SQL) and enterprise servers globally."[272]

December 5, 2014: Round Three Published - The GOP contacts cybersecurity companies and interested journalists to offer them more data. The links consist of just over 100GB of data and is titled "Financial data of Sony Pictures". It contains bank statements and account information, financial reports and forecasts, budget reports and receipts going back to 1998. It also contains licensing contracts with other major corporations, additional personal data and copies of driver's licenses and federal tax returns, [273]

---

[269] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

[270] Nichols, Michelle. "North Korea says "wait and see" when asked about Sony hacking." *Reuters*, December 1, 2014.

[271] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

[272] Ragan, Steve. "Sony's IT blueprints leaked by hackers." *CSO Online*, December 4, 2014. Located at: https://www.csoonline.com/article/2855005/sonys-it-blueprints-leaked-by-hackers.html

[273] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-

December 7, 2014: Some SPE employees receive threatening emails saying "It's false if you think this crisis will be over after some time. All hope will leave you and Sony Pictures will collapse. This situation is only due to Sony Pictures."[274]

December 8, 2014: Round Four Published – the fourth round of hacked data is published and consists of two large files totaling 2.8GB and including nearly 20,000 emails, including co-chairman Amy Pascal's email inbox and the President of Sony Pictures Television Steve Mosko's inbox, as well as 3,550 full contact details of names, emails and home addresses of Sony contacts. Accompanying the data is a message from the GOP claiming that they know nothing about the threatening email sent to employees and reiterating the demand for *The Interview* to be cancelled.[275] Amy Pascal's emails will reveal racist emails she wrote as well as emails where she belittles and mocks many of the Hollywood elite.

December 9, 2014: Sony Entertainment CEO Michael Lynton received an email FireEye's Kevin Mandia and forwarded it to the Sony Pictures Entertainment workforce. It included the following:

> This attack is unprecedented in nature. The malware was undetectable by industry standard antivirus software and was damaging and unique enough to cause the FBI to release a flash alert to warn other organizations of this critical threat. In fact, the scope of this attack differs from any we have responded to in the past, as its purpose was to both destroy property and release confidential information to the public. The bottom line is that this was an unparalleled and well-planned crime,[276] carried out by an organized group, for which neither SPE nor other companies could have been fully prepared.[277]

December 10, 2014: Round Five Published – the fifth data cache published included five 1GB links that contained the internal SPE business dealings with dozens of companies, potential partnerships, how Sony works with Internet Service Providers to monitor illegal downloads and more financial data.[278]

---

and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

[274] Ibid.

[275] Ibid.

[276] While the term "crime" was used by Mandia, since this cyberattack was for political purposes, the term "crime" is not the most appropriate. This cyberattack was coercive in nature and for political purposes and therefore it is considered not a crime where the purpose is money-making or simply destruction, but an act of political coercion.

[277] Lang, Brett. "Sony Hack 'Unparalleled and Well-Planned Crime,' Cyber Security Firm Says." *Variety*, December 6, 2014. See also, Danny Yadron. "Cyberattack on Sony is Called Sophisticated." *The Wall Street Journal*, December 7, 2014.

[278] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-

December 10, 2014: Round Six Published – on the same day as the fifth round, the GOP published the sixth round of data. This round consisted of some of the email of Leah Weil, Senior Executive Vice President and General Counsel for Sony Pictures Entertainment and included sensitive legal conversations and related emails with employee information.

December 11, 2014: Sony goes on record about the cyberattack and Amy Pascal apologizes for the discriminatory, derisive and objectionable communications that the data dump revealed.

December 13, 2014: Round Seven Published – the seventh data cache published included 6.45GB of uncompressed data consisting of 6,560 files in 917 folders. It includes business tracking files, business acquisition files and the working files of the former Sony Executive and VP of Worldwide Digital and Commercial Strategy.[279]

December 13, 2014: SPE demanded that media outlets stop reporting on the stolen and leaked data.[280]

December 14, 2014: Round Eight Published – the eighth data drop is another email spool, this time for the Senior Vice President, International Distribution for Sony Pictures Releasing International. The file was 5.53GB uncompressed and contained at least 72,900 emails in 7 primary folders. The bulk of the emails, 54,793, are in the Sent folder and dating back to May 20, 2008, with 12,414 in the inbox, and 4,276 in the deleted folder.[281]

December 14, 2014: Sony Pictures lawyer David Boies stated in a letter to media outlets that "in an ongoing campaign explicitly seeking to prevent SPE from distributing a motion picture, the perpetrators of the theft have threatened SPE and its staff and are using the dissemination of both private and company information for the stated purpose of materially harming SPE unless SPE submits and withdraws the motion picture from distribution."[282]

---

and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

[279] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

[280] Feeney, Nolan. "Sony Asks Media to Stop Covering Hacked Emails." *Time*, December 15, 2014.

[281] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

[282] Hesseldahl, Arik. "Here's Sony Lawyer's Letter Telling Publishers to Stop Publishing Leaks." *Vox*, December 14, 2014. Located at: https://www.vox.com/2014/12/14/11633802/sony-demands-end-to-publishing-leaks-from-stolen-data

December 15, 2014: Cybersecurity bloggers and journalists receive a cease-and-desist letter from SPE demanding that they stop publishing details about the company's recent hacking and delete any company data they collected that was published by the hackers that they may have downloaded to assess the breach.[283]

December 16, 2014: A threat was posted online on Pastebin along with a series of links "purporting to be provide more documents from the attack, labeled 'mlynton,' an apparent reference to Sony Pictures chief executive Michael Lynton."[284] The Pastebin threat invoked September 11, 2001 and was the following:

> Warning
> We will clearly show it to you at the very time and places "The Interview" be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to.
> Soon all the world will see what an awful movie Sony Pictures Entertainment has made.
> The world will be full of fear.
> Remember the 11th of September 2001.
> We recommend you to keep yourself distant from the places at that time. (If your house is nearby, you'd better leave.)
> Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment.
> All the world will denounce the SONY.

Later that day, the five largest theatre chains asked Sony to delay the film's release out of concern that the threats would deter movie-goers over the critical holiday season. At the time, Sony declined and planned to proceed with the film's Christmas Day opening.

December 16, 2014: Round Nine Published – as alluded to earlier in the day, the ninth release consisted of the email archive of the CEO of Sony Pictures, Michael Lynton. The two files totaled 1.84GB and contained email since November 2013, including 12,482 emails in the inbox, nearly 7,000 deleted emails and 7,085 contacts, among other data. The GOP claims to have 100 terabytes of data and as of December 16th they published about 235GB.[285]

---

[283] Krebs, Brian. "In Damage Control, Sony Targets Reporters." *Krebs on Security*, December 15, 2014. Located at: https://krebsonsecurity.com/2014/12/in-damage-control-sony-targets-reporters/ and accessed December 21, 2018.
[284] Peterson, Andrea. "Sony Pictures Hackers Invoke 9/11 While Threatening Theaters that Show 'The Interview'." *The Washington Post*, December 16, 2014.
[285] Cook, James. "Sony Hackers Have Over 100 Terabytes of Documents. Only Released 200 Gigabytes So Far." *The Business Insider*, December 16, 2014.

December 16, 2014: Later that day, following the threat and the ninth data dump, Sony Pictures canceled the New York premiere of the film scheduled for December 18, 2014, and the main stars, Seth Rogan and James Franco, canceled upcoming media promotion appearances.[286]

December 17, 2014: The threats and cyberattack campaign worked: other corporate entities were deterred from showing the movie, which was what North Korea had been requesting for months, and Sony decided not to release the film further. In response to speculation about releasing it on video-on-demand platforms, Sony Pictures said there will be "no further release plans of any kind."[287] This decision would change in the future, but it was the publicly declared decision as of December 17th

Although the Department of Homeland Security "dismissed the terrorist threat as lacking credibility,"[288] a spokesperson for one of the major theater chains noted that they wanted to ensure their patrons could enjoy entertainment in a safe environment and "must take threats against movie theatres very seriously and the recent unprecedented cyberattacks against Sony Pictures are no exception."[289] In an interview later, the SPE CEO noted that "a lot of the e-commerce players and large cable operators and satellite operators were concerned about getting hacked themselves" and therefore would not agree to release the film.[290]

Sony spokesperson declares that "Sony Pictures has no further release plans for the film"[291] and pulled the planned Christmas Day release of the film. "Sony executives briefly considered alternative options, including releasing it only via video-on-demand or on television, said a person at the studio."[292] Not only did the cinemas fear suffering violent attacks if they showed the film, Comcast Corporation, the giant cable provider did not want "to offer the movie on-demand due to its political sensitivity."[293] By the

---

[286] Calamur, Krishnadev. "Theater Cancels New York Premiere of 'The Interview'." *NPR*, December 16, 2014.
[287] Alexander, Bryan, Andrea Mandell & Elizabeth Weise. "No 'Interview' ... on any platform." *USA Today*, December 17, 2014.
[288] Fritz, Ben, Erich Schwartzel and Barret Devlin. "Sony Pulls Korea Film "The Interview;" U.S. Blames Pyongyang for Hack; Studio Scraps Dec. 25 Debut After Terrorist Threats Prompted Movie Chains to Skip Film." *The Wall Street Journal*, December 18, 2014.
[289] Yamato, Jen and Dominic Patten " 'The Interview' Yanked By Regal, AMC & Other Major Chains." *Deadline*, December 17, 2014.
[290] Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review*, July–August 2015.
[291] McNary, Dave. "Sony Has 'No Further Release Plans' for 'The Interview'." *Variety*, December 17, 2014.
[292] Fritz, Ben, Erich Schwartzel and Barret Devlin. "Sony Pulls Korea Film "The Interview;" U.S. Blames Pyongyang for Hack; Studio Scraps Dec. 25 Debut After Terrorist Threats Prompted Movie Chains to Skip Film." *The Wall Street Journal*, December 18, 2014.
[293] Fritz, Ben, Erich Schwartzel and Barret Devlin. "Sony Pulls Korea Film "The Interview;" U.S. Blames Pyongyang for Hack; Studio Scraps Dec. 25 Debut After Terrorist Threats Prompted Movie Chains to Skip Film." *The Wall Street Journal*, December 18, 2014.

afternoon, Sony scrubbed any mention of the film from its website[294] and released the following statement[295]:

> Statement From Sony Pictures
> In light of the decision by the majority of our exhibitors not to show the film The Interview, we have decided not to move forward with the planned December 25 theatrical release. We respect and understand our partners' decision and, of course, completely share their paramount interest in the safety of employees and theater-goers.
>
> Sony Pictures has been the victim of an unprecedented criminal assault against our employees, our customers, and our business. Those who attacked us stole our intellectual property, private emails, and sensitive and proprietary material, and sought to destroy our spirit and our morale – all apparently to thwart the release of a movie they did not like. We are deeply saddened at this brazen effort to suppress the distribution of a movie, and in the process do damage to our company, our employees, and the American public. We stand by our filmmakers and their right to free expression and are extremely disappointed by this outcome.

December 17, 2014: Fox's production company, New Regency, canceled its plans for a "film set in North Korea, in which Steve Carell was to have starred."[296] Regal Entertainment Group, a major cinema chain, released the following statement: "Due to the wavering support of the film The Interview by Sony Pictures, as well as the ambiguous nature of any real or perceived threats, Regal Entertainment Group has decided to delay the opening of the film in our theatres."[297]

December 19, 2014: The GOP published the following announcement:

> This is GOP.
> You have suffered through enough threats.
> We lift the ban.
> The Interview may release now.
> But be carful. (sic)
> September 11 may happen again if you don't comply with the rules.
> Rule #1: no death scene of Kim Jong Un being too happy
> Rule #2: do not test us again
> Rule #3: if you make anything else, we will be here ready to fight
> This is Guardians Of Peace.

---

[294] Ibid.
[295] Day, Mark. December 17, 2014. Located at: https://twitter.com/MarkDayNews/status/545340141817315328. See also, Michael Rothman and Jason Nathanson, "Sony Pulls the Plug on Dec. 25 Release of 'The Interview' After Threats." ABC News, December 17, 2014.
[296] Fritz, Ben, Erich Schwartzel and Barret Devlin. "Sony Pulls Korea Film "The Interview;" U.S. Blames Pyongyang for Hack; Studio Scraps Dec. 25 Debut After Terrorist Threats Prompted Movie Chains to Skip Film." *The Wall Street Journal*, December 18, 2014.
[297] Alexander, Bryan, Andrea Mandell & Elizabeth Weise. "No 'Interview' ... on any platform." *USA Today*, December 17, 2014.

December 21, 2014: According to Sony Pictures Entertainment's lawyer, David Boies, Sony reversed course and decided to distribute the film. He noted: "What Sony is trying to do is to get the picture out to the public but at the same time to be sure the rights of its employees and the rights of the movie-going public are going to be protected."[298]

December 23, 2014: CEO of Alamo Drafthouse Cinema, Tim League, announced on Twitter that "Sony has authorized screenings of THE INTERVIEW on Christmas Day. We are making shows available within the hour. #Victory."[299]

December 23, 2014: Crowdstrike's CEO, Dmitri Alperovitch, announced that its analysis of the attack resulted in North Korean attribution based on tracking this group since 2006. "We have also seen them engage in destructive attacks just like the Sony attacks, including the use of some of the same infrastructure. Some of the I.P. addresses that were used in the attack on Sony were also used in some of the past attacks. And parts of the malware, the malicious code that was used at Sony, has been shared across some of the previous attacks."[300] Mark Rogers of Cloudflare is less certain on attributing the attack to North Korea at this time.[301]

December 24, 2014 – January 18, 2015: Sony released "The Interview" for rental or purchase in the United States via streaming services including Xbox Video and YouTube.[302]

December 25, 2014: A total of 331 cinemas, largely independent and smaller cinemas, screened the opening of "The Interview."[303]

January 5, 2014: Sony CEO, Kazuo Hirai, makes his first public statement on the cyberattack and thanks "employees and partners for making "The Interview" available to

---

[298] Lee, Edmund. "You Will Get to See "The Interview," Sony Lawyer Says." *Vox,* December 21, 2014.
[299] Located at: https://twitter.com/alamodrafthouse/status/547435347882553344
[300] Ifill, Gwen. "Interview with Dmitri Alperovich and Mark Rogers." *PBS Newshour*, December 23, 2014. Located at: https://www.pbs.org/newshour/show/debating-north-koreas-involvement-sony-hack and accessed November 22, 2018.
[301] Ifill, Gwen. "Interview with Dmitri Alperovich and Mark Rogers." *PBS Newshour*, December 23, 2014. Located at: https://www.pbs.org/newshour/show/debating-north-koreas-involvement-sony-hack and accessed November 22, 2018.
[302] Lang, Brent. "'The Interview' Makes $40 Million Online and On-Demand." *Variety*, January 20, 2015.
[303] De Moraes, Lisa and Nellie Andreeva. "'The Interview' Release: 331 Theaters Aboard For Christmas Day." *Deadline*, December 24, 2014. Located at: https://deadline.com/2014/12/interview-christmas-release-theaters-deadline-looms-1201334671/ and accessed on December 14, 2020.

public audiences."[304]

January 13, 2015: In a rare press briefing, An Myong Hun, North Korea's deputy U.N. ambassador, denied that North Korea was responsible for the Sony Pictures Entertainment cyberattack. "My country has nothing to do with the Sony hacking."[305] He also noted that North Korea offered to undertake a joint investigation into the cyberattack.[306]

January 20, 2015: Sony reported total sales of approximately $40 million in rentals and sales for 'The Interview'. Sony spent roughly $75 million in production and promotion of the film.[307]

The Lazarus Group first appeared in 2009[308] and "came to substantial media notice in 2013 with a series of coordinated attacks against an assortment of South Korean broadcasters and financial institutions using DarkSeoul, a wiper program that overwrites sections of the victims' Master Boot Record."[309] The commercial cybersecurity industry assessed that the Lazarus Group is run by the North Korean government and the "…large-scale breach of Sony Pictures was attributed to Lazarus."[310]

February 4, 2015: After postponing the release of their 2014 earnings because the cyberattack took relevant systems offline, Sony Pictures provided the data on February 4, 2015, in a call with investors and analysts. At the time, SPE estimated the cost incurred for the cyberattack "to include approximately 15 million U.S. dollars (1.8 billion yen) for investigation and remediation costs."[311]

---

[304] Mochizuki, Takashi. "Sony Head Thanks Supporters in Hacking Attack." *Wall Street Journal*, January 5, 2015.
[305] Ford, Dana and Madison Park. "North Korea to U.S.: Show evidence we hacked Sony." *CNN*, January 14, 2015
[306] Ibid.
[307] Lang, Brent. "'The Interview' Makes $40 Million Online and On-Demand." *Variety*, January 20, 2015.
[308] "Lazarus Under the Hood." *Kaspersky Labs*, 2018. Located at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
[309] Tsing, William. "The Advanced Persistent Threat files: Lazarus Group." *MalwareBytes Labs*, March 12, 2019. Located at: https://blog.malwarebytes.com/threat-analysis/2019/03/the-advanced-persistent-threat-files-lazarus-group/ and accessed on January 15, 2021.
[310] Tsing, William. "The Advanced Persistent Threat files: Lazarus Group." *MalwareBytes Labs*, March 12, 2019. Located at: https://blog.malwarebytes.com/threat-analysis/2019/03/the-advanced-persistent-threat-files-lazarus-group/ and accessed on January 15, 2021.
[311] Contained in the financial statement itself is a note that the cyberattack prevented Sony Pictures Entertainment from providing the actual results for this statement so it is providing estimated results, to include an estimation of the costs associated with the cyberattack. "Consolidated Financial Results Forecast for the Third Quarter Ended December 31, 2014, and Revision of Consolidated Forecast for the Fiscal Year Ending March 31, 2015" *Sony News and*

February 5, 2015: Amy Pascal, co-chairman of Sony Pictures Entertainment, announced she was stepping down from her job after 27 years "after she endured a prolonged public relations disaster when hacked private e-mails showed her making racially charged jokes about the president"[312] among other embarrassing and inappropriate comments that were leaked. "Over 27 years, she rose through the management ranks and became known in Hollywood for her ability to create relationships with stars, directors and producers and to spot blockbuster films."[313] Although SPE claimed this transition was in the works for a while and was unrelated to the cyberattack, she later claimed that she had been fired due to the ramifications from the cyberattack.[314] Given the nature of the leaked data; it is highly unlikely that she would enjoy the same close relationships with stars, directors and producers after her mortifying and loathsome emails were leaked so, as she noted, stepping down from her position was a direct consequence of the leaked emails, despite SPE's attempt to claim otherwise.

October 2015 – April 2016: The class action lawsuit against Sony by former employees who were victims of the data breach was settled. The total bill for Sony will be about $15 million, including $8 million in damages to the plaintiffs, $4 million to maintain the ongoing identity protection via services from AllClear, and over $3 million to the attorneys.[315]

February 2016: Over a year after the cyberattack, security researchers across a number of cybersecurity companies working together determine that the Lazarus Group, run by the North Korean government, is responsible for the Sony Pictures Entertainment hack as well as over 45 malware families used in other prominent cyberattacks.[316] The CEO of Novetta, a leading cybersecurity firm, noted: "This wasn't a spontaneous capability that

---

Information. Tokyo, Japan. Located at: https://time.com/wp-content/uploads/2015/02/150204_sony.pdf and accessed on December 17, 2018.

[312] Kang, Cecelia. "Sony Pictures co-chair Amy Pascal steps down." *Washington Post*, February 5, 2015.

[313] Ibid.

[314] McNary, Dave. "Amy Pascal Talks Getting 'Fired,' Sony Hack and Angelina Jolie Emails in Candid Interview." *Variety,* February 11, 2015.

[315] Lieff, Cabraser, Heimann and Bernstein. "Sony Data Breach." Located at: https://www.lieffcabraser.com/privacy/sony-data-breach/. See also Dominic Patten. "Sony Hack Class Action Settlement Gets Final Approval." *Deadline,* April 6, 2016.

[316] Zetter, Kim. "The Sony Hackers Were Causing Mayhem Years Before They Hit the Company." *Wired*, February 24, 2016. As described in the article and highlighted earlier in this research, one technique used to identify commonalities across the malware families was "through the attackers' re-use of passwords, identical snippets of code, encryption keys, obfuscation methods for avoiding detection, command-and-control structures, and other telling code details and techniques. Through these commonalities, researchers compiled a massive toolkit of malware used by Lazarus that includes families of remote-access trojans, keystroke loggers, installers and uninstallers, spreading mechanisms, DDoS botnet tools, and hard drive wipers---such as the destructive wiper used in the Sony hack. Using these malware families, they then connected disparate attacks conducted over the last decade."

was developed a year prior to and in the months leading up to [the Sony hack]. It's an established capability that does provide insight into the nature of the attack and the fact that the perpetrators of this were well-organized and well-resourced."

Structured Focused Questions

Targets

What were the targets of the cyberattack?

The types of attack vectors used for the Sony Pictures Entertainment cyberattack were using various kinds of malware to gain access, defacing their internal websites, stealing data for a period of months or longer prior to Sony Pictures Entertainment being aware of the breach and, finally, strategically leaking the data in nine rounds of distribution on the internet. Since Sony Pictures Entertainment is a private, commercial entity, it was solely a soft, countervalue target.

The cyberattack rendered the network unable to be used on the morning of November 24, 2014. As Sony Pictures Entertainment would soon learn, not only were they unable to log on, but significant portions of the network had also been destroyed beyond any recovery ability. Employees were told that their email and network were down due to a hacking and to go home.[317] This is one more aspect of the financial losses for Sony from this incident; the time lost when their employees were unable to work.

Further, when the aggressors engaged in the cyberattack, they focused on stealing the email files of several leaders of Sony Pictures Entertainment and other prominent Sony executives, human resources files, credentials and passwords, and internal documents. The aggressors leaked this data out in chunks over the following weeks. This

[317] Zetter, Kim. "Sony Got Hacked Hard: What We Know and Don't Know So Far." *Wired*, December 3, 2014. Located at: https://www.wired.com/2014/12/sony-hack-what-we-know/ and accessed December 2, 2019.

served to increase the pressure on leadership, and intensify the audience costs, especially when the leaked emails of certain executives included salacious remarks about a number of well-known people.

Nature of Attack

What was the nature of the attack? How was the attack conducted?

The types of attack vectors used for the Sony Pictures Entertainment cyberattack was malware and the "adversaries embedded their custom malware with a hard-coded list of machines as well as credentials for administrators in the environment, "[318] which implies that the adversary spent time collecting information on and about the network before launching the cyberattack. which implies that there was a significant reconnaissance period before the initiation of the actual destructive attack itself.

"After the adversaries had taken all the information they sought, they dropped a wiper malware payload onto the network, which deleted data from hard drives and overwrote the boot sectors to prevent the machines from booting."[319] These were overwritten multiple times, meaning the data was overwritten and deleted repeatedly "to wipe the hard drives and make it impossible for even a sophisticated forensics

[318] Bradley, Tony. "CrowdStrike demonstrates how attackers wiped the data from the machines at Sony." *CSOnline*, February 4, 2015. Located at: https://www.csoonline.com/article/2880095/crowdstrike-demonstrates-how-attackers-wiped-the-data-from-the-machines-at-sony.html and accessed on December 3, 2018.
[319] Bradley, Tony. "CrowdStrike demonstrates how attackers wiped the data from the machines at Sony." *CSOnline*, February 4, 2015. Located at: https://www.csoonline.com/article/2880095/crowdstrike-demonstrates-how-attackers-wiped-the-data-from-the-machines-at-sony.html and accessed on December 3, 2018.

team to recover the data."[320] This cyberattack severely punished the victim by destroying their computer systems, deleting their data beyond any hope of recovery.

The ramifications from the attack and strategically leaked data were drawn out over several weeks in what appears to be a calculated decision to escalate the pain for the victim, so they would comply with the request. The attackers used different methods to distribute the data. For the release of what was likely the stolen movies, they used Pastebin, a favorite cloud repository for hackers, to post a package and links to files "hosted on four sites consisting of 26 parts, broken out into 25 1GB files, and one 894 MB rar file."[321] The attackers claimed to have over twelve terabytes of stolen data,[322] which is a massive amount of data, especially when a considerable amount is expected to be flat files, or text files.

The stolen and leaked data, in addition to the personally identifying information of tens of thousands of employees and actors, consisted of extremely candid emails between Sony employees, some of whom were executives. As noted above, these emails ranged from disparaging and belittling remarks about various actors to downright offensive and racist remarks. Beyond that, the documents also revealed questionable business practices.[323]

---

[320] Bradley, Tony. "CrowdStrike demonstrates how attackers wiped the data from the machines at Sony." *CSOnline*, February 4, 2015. Located at: https://www.csoonline.com/article/2880095/crowdstrike-demonstrates-how-attackers-wiped-the-data-from-the-machines-at-sony.html and accessed on December 3, 2018.
[321] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/ and accessed on November 30, 2019
[322] Ibid.
[323] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*,

Leadership as a Target, Potential Leadership Destabilization

Was leadership targeted?

Yes. The email communications among the Sony Pictures Entertainment leadership and senior executives were a key element in the audience costs and embarrassment the company suffered. Not only were email exchanges of some executives inappropriate and reprehensible, but some were also quite specific about negative feelings toward certain popular actors, which could make future work with those actors problematic or impossible. Stealing this sensitive information about the inner workings, private feelings and internal tensions among Sony Pictures leadership and then publicly publishing this information was a strategic decision to increase pressure on the leadership.

In the immediate aftermath of the cyberattack, Sony's Chief Executive Kazuo Hirai declared that he was confident in the performance of Sony Entertainment CEO Michael Lynton and Sony Pictures co-chairman Amy Pascal, and he did not place any blame on them for the cyberattack.[324] Amy Pascal would later step down from her position after nearly 30 years with Sony, claiming publicly that she had been fired from her position due to the fallout from the cyberattack campaign.[325] This leadership destabilization due to the coercive cyberattack that specifically targeted leadership is a

---

December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/ and accessed on November 30, 2019

[324] Fritz, Ben, Erich Schwartzel and Barret Devlin. "Sony Pulls Korea Film "The Interview;" U.S. Blames Pyongyang for Hack; Studio Scraps Dec. 25 Debut After Terrorist Threats Prompted Movie Chains to Skip Film." *The Wall Street Journal*, December 18, 2014.

[325] McNary, Dave. "Amy Pascal Talks Getting 'Fired,' Sony Hack and Angelina Jolie Emails in Candid Interview." *Variety*, February 11, 2015.

sizeable consequence. To be clear, she was fired because the content in her leaked emails meant she was unable to carry on with her duties, not because Sony Pictures was vulnerable to a cyberattack. Had those stolen emails never been leaked, she would not have to be starting over. "I'm 56, it's not exactly the time that you want to start all over again. But it's kind of great and I have to and it's going to be a new adventure for me."[326]

Attribution

What was the understanding about attribution at the time of the attack? Did this change over time?

There is now an abundance of linkages tying the Lazarus Group to North Korea, and as of February 2016, attributing the Sony Pictures Entertainment cyberattack to the Lazarus Group. However, even in 2014, given the totality of circumstances, Sony Pictures Entertainment, working with the cybersecurity private industry partners, assessed that the attack most likely came from North Korea and that it was related to the months of North Korea demanding that Sony Pictures Entertainment cancel the film release and the threats to cinemas who planned to screen the film.[327]. This was further substantiated by major cybersecurity professionals such as Dmitri Alperovitch, co-founder and CTO of the security firm CrowdStrike, who stated "there's no question that

[326] "Ex-Sony Chief Amy Pascal Acknowledges She Was Fired." *NBC News*, February 12, 2015. Located at: https://www.nbcnews.com/storyline/sony-hack/ex-sony-chief-amy-pascal-acknowledges-she-was-fired-n305281

[327] Fritz, Ben, Erich Schwartzel and Barret Devlin. "Sony Pulls Korea Film "The Interview;" U.S. Blames Pyongyang for Hack; Studio Scraps Dec. 25 Debut After Terrorist Threats Prompted Movie Chains to Skip Film." *The Wall Street Journal*, December 18, 2014.

North Korea is behind the Sony hack."[328]

Later, it became clearer that "Lazarus was initially known for its involvement in…a number of high-profile disruptive attacks, including the 2014 attack on Sony Pictures that saw large amounts of information being stolen and computers wiped by malware."[329] The Lazarus Group has honed its skills since approximately 2009, and their preparation "culminated in the 'scorched Earth' attack that struck Sony in November 2014 — a hack that wiped out many of the company's servers, resulted in the theft of terabytes of data, and ultimately brought the entertainment giant to its knees."[330]

As noted earlier in the examples of the Dukes, some hackers (nation-state and independent) will re-use code, re-use IPs, re-use sequence of actions, etc. because it is easy to re-use what works. Researchers from three major cybersecurity companies and a data analytics company, Symantec, Kaspersky Lab, AlienVault Labs, and Novetta, respectively, teamed up and "based on a years' worth of analysis… identified more than 45 unique families of malware used by the Lazarus Group. The researchers found these malware families primarily through the attackers' re-use of passwords, identical snippets of code, encryption keys, obfuscation methods for avoiding detection, command-and-control structures, and other telling code details and techniques."[331]

---

[328] Zetter, Kim. "Experts are Still Divided on Whether North Korea is Behind the Sony Attack." *Wired*, December 23, 2014. p. 6.
[329] Symantec Threat Hunter Team. "FASTCash: How the Lazarus Group is Emptying Millions from ATMs." *Symantec Enterprise Blog: Threat Intelligence*, November 8, 2018. Located at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware and accessed on December 8, 2019.
[330] Zetter, Kim. "The Sony Hackers Were Causing Mayhem Years Before They Hit the Company." *Wired*, February 24, 2016.
[331] Zetter, Kim. "The Sony Hackers Were Causing Mayhem Years Before They Hit the Company." *Wired*, February 24, 2016.

Symantec listed numerous links between Lazarus and software the group had left behind after launching an earlier, less virulent, version of the malware in February. One was a variant of software used to wipe disks during the Sony Pictures attack, while another tool used the same internet addresses as two other pieces of malware linked to Lazarus.[332] Looking back at 2014 from a 2017 cyberattack, Symantec researchers noted: "The same Internet connection was used to install an early version of [the 2017 attack] on two computers and to communicate with a tool that destroyed files at Sony Pictures Entertainment."[333] This is one method to reasonably link cyberattacks over time to a particular group.

According to Broadcom, a global technology company that designs and develops key components and infrastructure software solutions, an attack in 2016 repurposed a trojan horse that was used in the attack against Sony. The group Lazarus was linked to Backdoor.Destroyer,[334] a highly destructive Trojan that was… used in an attack against Sony Pictures Entertainment.[335]

---

[332] Menn, Joseph. "Symantec Says 'Highly Likely' North Korea group behind ransomware attacks." *Reuters*, May 22, 2017. Located at: https://www.reuters.com/article/us-cyberattack-northkorea/symantec-says-highly-likely-north-korea-group-behind-ransomware-attacks-idUSKBN18I2SH and accessed on December 6, 2019.

[333] Menn, Joseph. "Symantec Says 'Highly Likely' North Korea group behind ransomware attacks." *Reuters*, May 22, 2017. Located at: https://www.reuters.com/article/us-cyberattack-northkorea/symantec-says-highly-likely-north-korea-group-behind-ransomware-attacks-idUSKBN18I2SH and accessed on December 6, 2019.

[334] "Backdoor.Destover." *Symantec Security Center*, December 3, 2014. This security warning provides the background information on the trojan horse, what actions it performs, what IPs it connects to, and recommendations for system administrations.

[335] Johnson, A.L. "Endpoint Protection." *Broadcom*, May 26, 2016. Located at: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8ae1ff71-e440-4b79-9943-199d0adb43fc&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments and accessed on December 6, 2019.

At the time of the attack with the information known in the immediate aftermath, including the public statements from North Korean diplomats and various leadership, employing Healey's Spectrum of State Responsibility, would rank the attack between 4, State-Encouraged, and 9, State-executed.[336] Looking at the public statements from Sony Pictures, while the CEO noted that they were less concerned with who did than how to protect their employees, the attribution was likely between 5, State-shaped and 10, State-integrated. Combining this with Sharp's Known Coercer + Known Demand model, where he denotes the victim's certainty about coercer's identity as "more certain" for this case and therefore this was a case of cyber coercion, along with the technical information known at the time, the victim was able to surmount the attribution obstacle.

Audience Costs

What were the audience costs? What were the audience costs over time?

The audience costs were extensive. It included the fallout from Amy Pascal's reprehensible emails and the inappropriate emails concerning Hollywood elites culminating in her firing, to Sony being openly criticized for capitulating to the North Korean demands. There was outcry that a U.S.-based company was ceding to North Korean demands, therefore infringing on the First Amendment right to freedom of expression, and self-censoring.

[336] Healey's Spectrum of State Responsibility was created long after the 2007 Estonia attacks, but it is a useful tool to employ in assessing the cyberattack.

There were also audience costs with business associates, having their private information strewn across the internet, and their contractual agreements made public. "Firms have a financial incentive not to disclose intrusions that could undercut public confidence in their products and stock prices."[337] While recent attacks in 2020s have brought increased attention to the issue of cyber coercion (and, related, cybercrime via ransomware) as a 2011 McAfee white paper notes, "the public (and often the industry) understanding of this significant national security threat is largely minimal due to the very limited number of voluntary disclosures by victims of intrusion activity compared to the actual number of compromises that take place."[338] This is partly why the North Korean hacker's decision to publicly disclose the internal communications of Sony Pictures Entertainment was significant for the business-related audience costs that Sony Pictures Entertainment suffered. It could not simply and quietly dismiss the situation and move on; conversely, the embarrassing internal notes were splashed across all mediums, from Hollywood rags to cybersecurity research papers.

The audience costs faced by cyber coercion may differ from other forms of coercion given the nature of cyber and some of the advantages it provides to an aggressor. Unlike diplomatic threats or economic sanctions, in the case of Sony Pictures Entertainment, an advantage for the North Korean strategy is that SPE had the constant

---

[337] Nye Jr., Joseph. ""Nuclear Lessons for Cybersecurity?" *Strategic Studies Quarterly*, Winter 2011. p. 28.

[338] Alperovitch, Dmitri. "Revealed: Operation Shady RAT." *McAfee White Paper*, 2011. p. 3. The author was referring to a different type of intrusion, commonly referred to as a "RAT" or remote access tool, but the sentiment that commercial industry is less willing to publicly disclose hacking activities levied against them applies regardless of the type of technique used.

question of "what else is coming?" as the tranches of internal data were released over weeks and it suffered the repercussions to its employees, business associates, reputation and increased audience costs. Other methods of coercion, like land grabs, supporting an insurgency or air strikes may not apply when coercing commercial entities since they would likely invite a state response. That being said, "coercers seldom rely on one instrument at a time."[339] In the Sony Pictures case study, once a threat of physical violence was made over two weeks into the attack, despite being not a credible threat, secondary victims like the cinema chains took the threat more seriously because it was bolstered by the extensive cyberattacks. The original threat to SPE not to release the film followed by the destruction of the computer network, the release of internal business data, the doxing of personal information of employees and the non-credible threat of violence was all made excruciatingly public. This served to increase the audience costs and make it more difficult for SPE to back down in the face of North Korean demands for self-censorship.

Financial Costs

What were the financial costs? What were the financial costs over time?

The total financial cost of the cyberattack campaign against Sony Pictures Entertainment is estimated to be in the hundreds of millions of dollars. Experts estimate the overall cost to be about $200 million, including $80 million in direct damages and

[339] Byman, D and M Waxman. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might.* UK: Cambridge University Press, RAND, 2002. p. 120.

more than $120 million in indirect damages (e.g. class action lawsuits from Sony employees for mishandling personal information, legal fees, remediation costs, leaked trade secrets, etc.)[340] Sony Pictures Entertainment, on its Third Quarter Financial Statement, ending December 31, 2014, estimated the cost "to include approximately 15 million U.S. dollars (1.8 billion yen) for investigation and remediation costs relating to the …cyberattack."[341] Sony Pictures spent $44 million to make *The Interview* and about $30 million more to market it. Since it was distributed on a severely limited theatre release and on video, it only brought in only $2.8 million at the box office and $15 million across all digital streaming services in its opening, far below the original expected revenue.[342] Overall, Sony reported total sales of approximately $40 million in rentals and sales for 'The Interview' after spending nearly $75 million in production and promotion.[343]

---

[340] Brinded, Lianna. "The Interview Tipped to Cost Sony Pictures $200 Million Following Hack and Cancellation." *International Business Times*, December 18, 2014.

[341] Contained in the financial statement itself is a note that the cyberattack prevented Sony Pictures Entertainment from providing the actual results for this statement so it is providing estimated results, to include an estimation of the costs associated with the cyberattack. "Consolidated Financial Results Forecast for the Third Quarter Ended December 31, 2014, and Revision of Consolidated Forecast for the Fiscal Year Ending March 31, 2015" *Sony News and Information.* Tokyo, Japan. Located at: https://time.com/wp-content/uploads/2015/02/150204_sony.pdf and accessed on December 17, 2018.

[342] Tassi, Paul. "'The Interview' Made $15M At the Digital Box Office On A $44M Budget." *Forbes*, December 29, 2014.

[343] Lang, Brent. "'The Interview' Makes $40 Million Online and On-Demand." *Variety*, January 20, 2015.

Pressure on Leadership

What was the pressure on leadership during the cyber crisis?

There was significant pressure on the leadership of Sony Pictures during the cyberattack campaign. This came in a number of forms including: personal pressure due to the embarrassment of having their own disgraceful emails exposed, pressure to remove the malware from their systems, pressure to reconstitute the servers and data that were wiped, where possible, pressure to get everyone back to a productive environment, pressure to ensure that the employees are cared for now that their personal data was exposed, pressure to stay on a production schedule and pressure to minimize the considerable public relations fallout from this cyberattack campaign.

When the threat of violence was made on December 16th against any cinema showing the movie, the major theatre companies decided that this unsubstantiated threat exceeded their comfortability and refused to show the film. This also put pressure on Sony's leadership; if they demanded theatres show the film and a violent act occurred, they would be responsible. However, if they capitulated to the threat, they were letting the North Korean's coerce them. The major theatre chains simply refused to show the film, so Sony's executives decided to cancel the film and then changed that decision to a release to independent theatres and on video-on-demand. They did not fully acquiesce to the North Korean demands, but instead released the movie in a much more limited fashion.

Weeks later, several computers at Sony Pictures Entertainment were still off for

fear of re-infection.[344] This was a devastating attack for the company, for the company's reputation, losing company proprietary information and unreleased films, revealing poor security practices regarding the handling of personally identifying information, and costing the company millions. All due to one film that was perceived to be insulting to the Dear Leader.

The CEO of the cybersecurity firm Crowdstrike noted:

> Another thing that makes this unprecedented is the action that the theater chains and studios are taking to suppress release and stop production of movies about North Korea. This is the first time that I can remember where a victim of a cyberattack has been forced to take an action in the physical world against their will, which sets a very dangerous precedent.[345]

George's seven conditions as structured focused questions:

Clarity of the Objective

What was the victim's understanding of the clarity of the objective?

In this case study, the victim anticipated problems with North Korea, perhaps not to the extent that bore out, but they were aware of the aggressor's objective of getting the film suppressed. Subsequent to the cyberattack, by December 14, 2014, the company was quite clear that they were being coerced into not releasing the film. The Sony Pictures lawyer, David Boies sent a letter to a number of media outlets threatening them

---

[344] Cieply, Michael and Brooks Barnes. "Sony's Dirty Laundry, For All to See." *The New York Times*, December 11, 2014.

[345] Alperovitch, Dmitri. "Unprecedented Announcement by FBI Implicates North Korea in Destructive Attacks" Crowdstrike, December 16, 2014. Located at: https://www.crowdstrike.com/blog/unprecedented-announcement-fbi-implicates-north-korea-destructive-attacks/ and accessed December 20, 2018

with liability if they published stories on the leaked emails, but the letter is illuminating is its understanding of the clarity of the objective. In his letter Mr. Boies noted the following:

> "in an ongoing campaign explicitly seeking to prevent SPE from distributing a motion picture, the perpetrators of the theft have threatened SPE and its staff and are using the dissemination of both private and company information for the stated purpose of materially harming SPE unless SPE submits and withdraws the motion picture from distribution."[346]

This shows that Sony Pictures was unambiguously clear about the demand from the aggressor.

Strength of Motivation of the Coercer

What was strength of motivation of the coercing power?

The coercing power, North Korea, was strongly motivated because it interpreted the film as a direct insult and a threat to the North Korean leader. North Korea had been publicly speaking out against the film for six months prior and felt so strongly, its representative to the UN sent a letter to the UN General Secretary, Ban Ki-moon, demanding that the United States ban production and distribution of the film, claiming that allowing its production is sponsoring terrorism and an act of war.[347] Evidently, North Korea felt extremely motivated to prevent the release of the film.

---

[346] Hesseldahl, Arik. "Here's Sony Lawyer's Letter Telling Publishers to Stop Publishing Leaks." *Vox*, December 14, 2014. Located at: https://www.vox.com/2014/12/14/11633802/sony-demands-end-to-publishing-leaks-from-stolen-data

[347] Beaumont-Thomas, Ben. "North Korea complains to UN about Seth Rogen comedy The Interview." *The Guardian*, July 10, 2014. Located at:

Asymmetry of Motivation

What was the asymmetry of motivation between the adversaries?

There appeared to be an asymmetry of motivation between the adversaries. The North Koreans sought to disrupt the release of the film and pursued a strategy that would result in extreme punishment for Sony Pictures Entertainment for the perceived disrespect of the Kim Jong-un. In the words of the SPE CEO, he was mainly focused on how to keep the business going, keep production on schedule, tend to his employees, and figure out how to reconstitute his computer networks more than he was concerned with who executed the attack.[348] For North Korea the production of this film was an act of war and terrorism; to Sony Pictures this was a terrible, costly, embarrassing cyberattack, but they were not willing, at first, to immediately cancel the film. Their first actions were focused on providing information and assistance for their employees and, second, to legally compel media outlets to stop reporting on the leaked internal emails. There was a complete asymmetry of motivation. Following the threat of violence, the film and its promotion events were cancelled and, later, a different decision was made for a limited release and release via video-on-demand.

Sony Pictures Entertainment and the Sony parent company cared about the North Korean rhetoric when tensions began to increase the summer prior to the planned release of the film. That is why SPE agreed to costly digital edits to reduce the visual carnage

---

https://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco

[348] Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review*, July–August 2015.

associated with the assassination of the North Korean leader. It is also why the SPE CEO reached out to a major think tank for its perspective on North Korea's bluster and whether SPE needed to be more concerned about the narratives.

Initially, when the cyberattack was discovered on November 24, 2014, SPE cared about the demand, but in the chaos of trying to discover the extent of the attack, the extent of the stolen data, identifying and contracting with FireEye for assistance, it is not clear how quickly SPE was able to link the cyberattack to the North Korean demands, but certainly by November 28, 2014, it was being publicly floated.[349]

SPE received threatening messages warning that its internal data would be released. As the stolen data began to be published, pressure on leadership increased. The SPE CEO noted that he was dealing with several things at once including keeping the business running while setting up analog communications, dealing with employees concerned that their private information would be splashed across the internet and potential identity theft, figure out how to make payroll without working computer systems and of course managing the flood of press requests and stories coming out about the internal emails.[350] Looking back on the cyberattack nearly nine months later, the SPE CEO noted "I actually haven't been concerned about who did this. I've been more concerned about getting the business up and running and making sure folks here feel

---

[349] Hesseldahl, Arik. "Sony Pictures Investigates North Korea Link In Hack Attack." *Vox,* November 28, 2014. Located at: https://www.vox.com/2014/11/28/11633356/sony-pictures-investigates-north-korea-link-in-hack-attack

[350] Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review,* July–August 2015.

calm enough and secure enough to keep on with their jobs." This statement neglects to mention how the CEO felt about the threat of physical violence and what weight that carried in his decision on December 21, 2014 to reverse and release the film on a limited distribution and via streaming. It is likely that the outrage from customers voicing their anger that Sony was acquiescing to North Korea's demand to self-censor increased the audience costs to a level that affected the motivation of the leadership to change their original decision.

Victim Understanding of Urgency

What was the victim's understanding of the coercer's sense of urgency?

Sony understood North Korea's demand and its sense of urgency, beginning the summer prior to the planned movie release. When the leaking of the stolen data from the cyberattack began a month prior to the planned release date, the SPE CEO was clear about the aggressor's sense of urgency. This urgency was underscored by the subsequent threat of violence made a few weeks after the initial leak of stolen data.

Adequate Domestic and International Support

Is there adequate domestic and international support for the victim and the coercer?

The victim in this case study was a commercial entity, a multi-national company, so its domestic support came in several forms. This included several Hollywood elites who were outspoken that a company should not be attacked and bullied into muzzling its

free speech rights to make this satirical film.[351] And, on the other side, the President of the United States said it was a mistake for the company to cancel the film, citing that a dictator should not be able to "impose censorship in America."[352] International support for Sony Pictures is difficult to measure since countries did not offer any public statements of support, however, Sony's parent company located in Japan obviously did. Since North Korea is a closed, authoritarian state, attempting to measure domestic support for the regime's activities is a meaningless exercise since approval ratings for the government's activities is artificially dictated by the government. During the 2014 timeframe, this research did not uncover any public, international support for North Korea's actions.

Fear of Unacceptable Escalation

What is the opponent's (victim's) fear of unacceptable escalation?

This cyberattack revealed the private, internal emails of the company's leadership and they were ugly. As these documents were leaked and the links posted, Sony Pictures Entertainment had no way of knowing if the leaked tranche of documents would be the first of five or the first of ten tranches or if the links posted consisted of everything that was stolen or if there was more damaging information to come to light. Given the

---

[351] "A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

[352] Peralta, Eyder. "Obama Says Sony Should Not Have Pulled Film Over Threats." *National Public Radio,* December 19, 2014

repercussions from the initial batches that were posted, there was considerable pressure on the leadership at Sony Pictures Entertainment to not escalate further. Beyond the public embarrassment, the information systems at Sony were suffering in the aftermath of the attack, with some computers completely unusable and significant data deleted, and the business itself was in jeopardy of failing to maintain its financing and production schedule. Sony Pictures Entertainment was fearful of further escalation, not knowing what else was stolen and could be leaked or what other systems had been compromised and the data could be destroyed remotely but were equally concerned about protecting their employees.[353]

As for the decision from the major theatre chains not to air the film, part of this decision was that they did not want to become a target of cyberattacks themselves, according to the statements from the SPE CEO and from a spokesperson for one of the five major cinema chains in North America on December 17, 2014. This represents secondary deterrence; that is, similar to the movie studios that cancelled future films with a North Korean angle, the cinema chains were not the direct targets of the cyberattack, but in changing their behavior due to the cyberattack and subsequent threat of violence, they are a secondary coercee who chose to change their behavior lest it become the next North Korean cyberattack victim, or worse.

[353] Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review*, July–August 2015.

Clarity on Terms for Settlement

What is the clarity concerning precise terms of the settlement of a crisis for the victim and the coercer?

Sony Pictures dismissed the terms of the coercion settlement, at first, but as the attack progressed and additional internal documents were leaked, it clearly understood that the purpose of the attack was to prevent the release of a movie that was critical of the North Korean leader. The letter from the SPE lawyer clearly articulates that SPE understood the terms for settlement.

Conclusion

The conventional wisdom says that Sony Pictures "won" this cyber confrontation. After all, *The Interview* was produced and was shown in some theaters and on video-on-demand. However, the conventional wisdom is wrong, too narrowly focused on the binary of winning/losing and too limited temporally. The most interesting aspect is to uncover not only *why* and *how* it is wrong, but what the data proves about this cyber coercive act, what the conventional wisdom ought to be regarding the outcome, and what factors led to this outcome.

Sony Pictures Entertainment was on the receiving end of extraordinary cyber pressure, later coupled with a threat of violence, and this resulted in a series of significant decisions at Sony Pictures that led to Sony Pictures capitulating partially to the North Korean demand. Beyond that, there was secondary deterrence in the form of other Hollywood studios cancelling North Korean-focused movies and large theatre chains refusing to show the film for fear of incurring the North Korean cyber wrath and suffering a similar cyberattack or, worse, being subjected to actual physical violence.

Sony Pictures suffered the "gradual turning of the screw"[354] with the cascade of cyber leaks that included damning, damaging or embarrassing information in each tranche released. The cyberattack primed the landscape and put Sony on the defense, so when the threat of physical violence came, even though law enforcement did not find it to be a credible threat, it caused a high level of consternation and caused several related

[354] George, Alexander. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War.* Washington, DC: United States Institute of Peace Press, 1991. p. 8.

companies to change their decision-making regarding *The Interview* as well as other films with a North Korean plot. Effectively, the cyberattack and the additional threat of violence resulted in a secondary deterrence; no company wanted to take the chance that they might be the next cyberattack victim, jeopardizing all their internal security, financial documentation, personal emails, employee files, business contracts, and computer networks. Further, although the threat of physical violence was determined not to be a credible threat, on the heels of the extensive Sony Pictures cyberattack, no company wanted to take the chance.

The threat of violence alone may not have resulted in the cinema closings, but on the heels of the massive cyberattack, it signaled that the aggressor had a significant commitment to the demand and was an extremely motivated actor. Simply, the cyberattacks made this otherwise relatively implausible threat more credible to the business owners. The question was: was North Korea motivated enough to carry out a physical attack at a cinema? No major theatre chain operator wanted to find out. The combination of the cyberattack, the nature of the cyberattack and the threat of physical violence that amplified the effectiveness of the coercion resulted in Sony Pictures and several related companies changing their behavior, changing their decision-making and those changes significantly reduced the distribution of the film. This of course resulted in less earning for the film than originally anticipated along with the hefty remediation costs for the destroyed systems from the cyberattack.

Sony had other levers of pressure to exert over the theatres in an effort to convince them to air *The Interview*, if they were motivated to do so. Sony Pictures could

monetarily penalize them, or possibly threaten to withhold future blockbusters, or give exclusivity to one chain over others to entice them to air *The Interview,* but they did not exercise these options and allowed the limited release in independent theatres.[355] Sony Pictures was not sufficiently motivated to pressure the distributors and understood the distributors fear of incurring additional cyberattacks against their companies if they agreed to air the film.

The cyberattack against Sony was successful in compelling Sony Pictures and the theatre companies to change their decision. As well, it served to deter Sony Pictures from pressuring these companies and deterred other studios from moving forward with North Korea-related films out of fear of drawing the ire of North Korea and causing additional future cyberattacks. That is a significant factor and part of the reason why the conventional wisdom that "Sony won" is terribly incorrect. American companies restrained their decisions about future activities based on the fear that their actions could result in making them the next cyberattack target, or physical attack target, and, instead, made a decision that would not incur North Korea's wrath. This coercive cyberattack resulted in changing the behavior and effectively deterring the activities of multiple American companies.

The North Korean strategy to slowly release information and destroy the SPE computer networks put pressure on SPE leadership to cancel the film, which is what originally occurred. However, with the subsequent releases of stolen data, the increased

[355] Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review,* July–August 2015.

importance and scandal of the information released, and the ensuing threat of physical violence, the audience costs for SPE reached a level that SPE could not ignore. That is, Americans were extremely upset that a U.S.-based company was attacked by a foreign country and forced to self-censor, and some Hollywood elites were extremely outspoken on the subject. So, SPE leadership reversed its decision and moved to release the film through the means it had available. This is why the conventional wisdom is that Sony Pictures "won" this conflict, however, this research has shown that it is not the full story.

The SPE CEO also noted that, in light of his experience with the cyberattack, that he and "everybody is more cautious about what they put in e-mail, and the instinct nowadays is more often to pick up the phone or meet in person, particularly when you're talking about difficult stuff."[356] Another way of looking at this firsthand account from the victim is that, in the future, he and his associates have permanently changed their behavior online due to the North Korean cyberattack. That is not a failure for North Korea, that is a long-term behavior change and a successful outcome for Pyongyang's strategy.

This case study provides ample avenues for additional policy research and development, as will be discussed in the section on future policy work. Areas and topics include disincentives for targeting commercial targets, penalties for engaging in hack and leak tactics of commercial entities and cyberattack disclosure requirements.

---

[356] Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review,* July–August 2015.

CHAPTER 5: ESTONIA CASE STUDY

A fight over the relocation of a Red Army statue and World War II-era Russian soldier remains in April 2007 ignited tensions resulting in a two-phase Russian cyber operation against Estonia, one of the most digitally-reliant countries in Europe at the time. Coupled with a few days of public demonstrations and rioting, the Russian cyberattacks lasted for weeks and successfully suspended online and ATM services of Estonian banks, inhibited the government's ability to communicate among agencies and the news media were unable to produce the news; the entire country had been targeted.[357] While it was a momentous show of force by Russia, it was not successful in achieving the goal — Estonia did not change its behavior and went ahead and relocated the statue and the remains. Moreover, this attack demonstrated to the Estonians, and to all of Europe, how a country could be paralyzed by cyberattacks and therefore greater investment in cyber security was required. While it was a tactical and technical success for Russia, Estonia turned it into a strategic advantage for the Estonians. The conventional wisdom is that

> The three-week long DDoS achieved several different outcomes including the expression of [Russian] diplomatic discontent; the flexing of "virtual" muscles; and the capturing of the Estonian government's attention. …The DDoS did not target a sector or a specific organization but a nation's information infrastructure… [and] …the world was witness to what it had long heard about but up until this point had never seen – cyberattacks shut down a country's information infrastructure.[358]

---

[357] Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*, August 21, 2007. Accessed via https://www.wired.com/2007/08/ff-estonia/ on October 26, 2018.
[358] Iasiello, Emilio. "Cyber Attack: A Dull Tool to Shape Foreign Policy." *2013 5th International Conference on Cyber Conflict*, K. Podins, J. Stinissen, M. Maybaum, eds. Tallinn: NATO CCD COE Publications, 2013.

"Cyber warriors tend to see that Estonia lost in 2007 because of a focus on technical impact rather than the more strategic view that winning means achieving better national security outcomes."[359] The technical management throughout the cyberattack duration was superior and

> clearly from a tactical standpoint, the DDoS attacks against the Estonian information infrastructure were an unqualified success. For three weeks, Estonia was the target of these attacks. Each time there was a pause in the activity, it would resurface soon after stronger and more potent than earlier iterations. What's more, the attackers constantly tweaked their malicious server requests to evade filters.[360]

Russia clearly understood that the tactical effect was useful for its goals since it employed similar techniques the following year against Georgia as part of its hybrid warfare strategy combined with kinetic attacks.[361] However, these assessments, once again, framed a cyber coercive act too narrowly, focused on the binary of winning/losing while also limiting the time period examined. This case study will show the additional variables involved in failing to coerce a victim to change its behavior over time including audience costs, financial costs, a lack of asymmetric motivation and no fear of unacceptable escalation.

---

[359] Healey, Jason. "Winning and Losing in Cyberspace." In 2016 8th International Conference on Cyber Conflict Cyber Power, N. Pissanidis, H. Rõigas, M. Veenendaal, Eds. Tallinn: NATO CCD COE Publications, 2016.
[360] Iasiello, Emilio. "Cyber Attack: A Dull Tool to Shape Foreign Policy." *2013 5th International Conference on Cyber Conflict*, K. Podins, J. Stinissen, M. Maybaum, eds. Tallinn: NATO CCD COE Publications, 2013.
[361] Interview with Toomas Hendrik Ilves, President of Estonia, 2007 – 2016. "10 Years of Cyber Estonia: What will the Next Decade Bring?" *Center for Strategic and International Studies*, November 6, 2017.

Background

In the Spring of 2007, Estonia faced an unprecedented cyberattack campaign against several of its national critical functions to include the financial industry and government services, spanning 22 days, from April 26, 2007, to May 19, 2007. Researchers and academics suggest that Estonia "lost" the fight, but that is an artificially narrow understanding of the conflict focused solely on the tactical cyberattack and ignores the significant strategic cyber developments that arose from the conflict and damaged the relative power of the adversary in the cyber realm in Estonia. That view also ignores the secondary effects of this incident that served as a wake-up call for Europe to not only recognize the cyber threat, but to act meaningfully to improve knowledge sharing and defense, to include building a NATO Cyber Centre of Excellence in 2008 based in Tallinn. Given the strategic and operational changes that occurred in Estonia and for NATO in the aftermath of the 2007 cyberattacks, Estonia turned the experience of the short-term crippling cyberattacks into a long-term strategic advantage. The event served as a rallying cry in the West to commit resources and expertise against the priority of the Russian cyber threat. That being said, the incident also allowed Russia to exercise its capabilities, learn efficiencies and refine them. It used similar tactics in its conflict with Georgia the following year.

After several months of publicly proposing the move, the Estonian government decided to relocate a Soviet-era war monument. Estonia has a rich and colorful history in its relationship with Russia. At one time it was part of the Russian Empire, first declaring its independence in 1918, after the collapse of the Russia Empire. It then became a

Soviet republic following a tense period from 1939-1944 until 1991, when it declared its independence once again.

On April 26, 2007, the Estonian government in Tallinn began initial preparations to relocate the Soviet-era national monument dedicated to the Red Army, "the Bronze Soldier" statue along with the remains of a dozen soldiers buried at the monument and elaborate grave marker, from the center of Tallinn to a nearby military cemetery. The "bronze soldier in Soviet Army uniform, head uncovered, and rifle slung on his back with barrel pointing to the ground, stands at ease."[362] This monument was originally erected in 1947 as a tribute to Soviet soldiers who died in World War II and its proposed relocation was strongly opposed by the ethnic Russian population living in Estonia and by the Russian government[363] whose foreign ministry called the plan a "blasphemous, idea and a blatant mocking of the memories of Red Army soldiers."[364] This decision to move the Bronze Soldier statue followed a series of public protests, sometimes violent, in Tallinn and outside the Estonian embassy in Moscow that occurred over several months. It was a sensitive topic for ethnic Russians and ethnic Estonians for different reasons, complicated by a convoluted history concerning statues in Tallin.

"After winning WWII, the Soviets blew up the monument dedicated to Estonian

---

[362] Mardiste, David. "Russia to Estonia: Don't Move Our Statue." *Reuters,* January 25, 2007. https://www.reuters.com/article/us-estonia-russia-statue/russia-to-estonia-dont-move-our-statue-idUSL2378719620070125 and accessed on November 11, 2019.
[363] Tapon, Francis. "The Bronze Soldier Explains Why Estonia Prepares For a Russian Cyberattack." *Forbes,* July 7, 2018. https:// www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/?sh=59f777da98c7 and accessed on November 14, 2019.
[364] Mardiste, David. "Russia to Estonia: Don't Move Our Statue." *Reuters,* January 25, 2007. https://www.reuters.com/article/us-estonia-russia-statue/russia-to-estonia-dont-move-our-statue-idUSL2378719620070125 and accessed on November 11, 2019.

independence"[365] and replaced it with a wooden structure. This wooden structure was destroyed by two Estonian teenagers who were eventually caught and sentenced to work in Soviet labor camps for years. It was at this point, in 1947, that the Soviets installed the Bronze Soldier statue to commemorate their success in WWII. In 1998, the two Estonian teenagers, then in their 60's, were awarded Estonia's highest medal. In Estonia, the suggestion to move the Bronze Soldier statue was attached to a complicated and storied history of representation, occupation, and marginalization.

For the Russians, the Bronze Soldier statue represented the heroic efforts and sacrifices by Russians during World War II and was a symbol of the identity for the minority ethnic Russians still living in Estonia. It is also a rallying point for every May 9th when Russians gather at the Bronze Soldier statue to commemorate Russia's Victory in Europe World War II celebration.[366] The proposal to move the monument and the associated remains was seen as an attack on the minority community and an attempt to marginalize the ethnic Russian identity in Estonia. The proposal provoked a passionate and aggrieved response that came in the form of violent protests lasting several days in April 2007.[367] For the Estonians, the Bronze Soldier statue was a symbol of unwanted

---

[365] Tapon, Francis. "The Bronze Soldier Explains Why Estonia Prepares for a Russian Cyberattack." *Forbes,* July 7, 2018. https:// www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/?sh=59f777da98c7 and accessed on November 14, 2019.

[366] Mardiste, David. "Russia to Estonia: Don't Move Our Statue." *Reuters,* January 25, 2007. https://www.reuters.com/article/us-estonia-russia-statue/russia-to-estonia-dont-move-our-statue-idUSL2378719620070125 and accessed on November 11, 2019. See also, Tapon, Francis. "The Bronze Soldier Explains Why Estonia Prepares for a Russian Cyberattack." *Forbes,* July 7, 2018. https:// www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/?sh=59f777da98c7 and accessed on November 14, 2019.

[367] "Tallinn tense after deadly riots." *BBC News,* April 28, 2007.

Soviet occupation and, for some, an emblem of ongoing tensions with ethnic Russians still living in Estonia.

Cyberattack

The cyberattacks Estonia suffered in 2007 were a watershed moment in the history of hostile cyber actions due to the breadth and depth of the attack. Estonia endured cyberattacks lasting over three weeks, consisting of two distinct phases, with the first phase, considered the "emotional response," beginning on April 26, 2007, and lasting until April 29, 2007 and the second phase, "the main attack," lasting from April 30, 2007 to May 19, 2007.[368] The cyberattacks targeted Parliament, various government ministries and agencies, banks and other economic sector businesses, private companies, the news media, "mail servers, DNS servers and backbone routers."[369]

The Phase I attacks were unsophisticated, targeting government webpages for defacement or relatively simple denial-of-service (DoS) attacks. The main attack, Phase II, was advanced, massive and coordinated and relied heavily on botnets. "The most dangerous ones were Distributed Denial of Service (DDoS) attacks against some of the components of the critical information infrastructure – against the backbone routers of data communications network and DNS servers."[370] Two weeks into the attacks, on May 10th, the attacks on the banks began which meant banking services were unavailable

---

[368] Viira, Toomas. "Cyber Attacks Against Estonia - Overview and Conclusions." *Information Technology in Public Administration of Estonia - Yearbook 2007*. Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008. p. 72. The author of the article was the information security manager in the Estonian Informatics Centre in 2007.
[369] Ibid.
[370] Ibid.

locally for a period of time and "restrictions were applied for accessing Internet banking services from other countries."[371] Some attacks only disrupted operations for a few minutes at a time while others interrupted access for hours.

To fully understand the extent of disruption caused by these cyberattacks, it is essential to understand how much Estonians relied upon their digital infrastructure for their daily lives in 2007. Estonia decided in the 1990s to invest significantly in digital infrastructure to become one of the most technologically advanced countries. By 1996, 90 percent of the Estonian population used the internet regularly; by 2000 the government cabinet meetings were online, by 2002 Estonia employed a mandatory digital ID card, and by 2007, Estonia offered comprehensive e-voting.[372] For this small Baltic nation that was extremely digitally-dependent for its economic health and growth, as well as its government and societal functions, a multi-week paralyzing attack was a significant blow to the country. According to Rain Ottis, a scientist at the NATO Cooperative Cyber Defence Centre of Excellence in 2008, "Estonia is highly networked, so a wide scale attack on the availability of public digital services has a significant effect on the way of life of ordinary citizens and businesses alike. …these cyberattacks… should be considered a threat to national security.[373] The Director of IT security at the Estonian

---

[371] Ibid.

[372] Statistics provided by e-Estonia.com. According to Rainer Kattel and Ines Mergel in "Estonia's Digital Transformation," the "Estonian e-government infrastructure and its success rest on two main pillars, both introduced in 2001, that essentially create a digital state and digital citizens: the data infrastructure X-Road and a compulsory national digital ID." Article is in *Great Policy Successes.* Compton, Mallory E.; Hart, Paul. Oxford : Oxford University Press, 2019.

[373] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia. 2008. As of 2021, Estonia conducts 99% of its government services online.

Ministry of Defence at the time, Mihkel Tammet, remarked:

> "Of course [websites] can be put up again, but they can be attacked also again. Estonia depended largely on the internet because of the country's 'paperless government' and web-based banking. If these services are made slower, we, of course, lose economically.[374]

The Estonian Defense Minister at the time, Jaak Aaviksoo, noted:

> The attacks were aimed at the essential electronic infrastructure of the Republic of Estonia. All major commercial banks, telcos, media outlets, and name servers — the phone books of the Internet — felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation.[375]

The then-President Toomas Hendrik Ilves of Estonia said "it was unheard of, and no one understood what was going on in the beginning"[376] when Estonians first discovered that online media, government websites and banking resources, among others, were all inaccessible. On September 25, 2007, in an address to the United Nations General Assembly, Estonia's President made a plea that:

> Cyberattacks are a threat not only to sophisticated information technological systems, but also to a community as a whole.… The threats posed by cyber warfare have often been underestimated since, fortunately, they have so far not resulted in the loss of any lives.… In addition to concrete technical and legal measures for countering cyberattacks, governments must morally define the cyber violence and crime, which deserve to be generally condemned just like terrorism or the trafficking in human beings.[377]

---

[374] "The cyber raiders hitting Estonia." *BBC News*, May 17, 2007. Located at: http://news.bbc.co.uk/2/hi/europe/6665195.stm and accessed on November 23, 2019.
[375] Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*, August 21, 2007. Accessed via https://www.wired.com/2007/08/ff-estonia/ on October 26, 2018.
[376] Tamkin, Emily. "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy*, April 27, 2017.
[377] Ilves, Toomas Hendrik. 'Address by the President of Estonia' (62nd Session of the United Nations General Assembly, New York, September 25, 2007. https://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf

When asked to reflect on the cyberattack campaign ten years later, former-President Ilves noted: "Looking back on it, it was the first, but hardly the last case in which a kind of cyberattack … was done in an overtly political manner."[378] He would later describe the cyberattacks as 'Web War One.'[379]

[378] Tamkin, Emily. "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy*, April 27, 2017.
[379] Ilves, Toomas Hendrik. 'Address by the President of Estonia' (67th Session of the United Nations General Assembly, New York, September 26, 2012. https://vp2006-2016.president.ee/en/official-duties/speeches/7991-address-by-h-e-toomas-hendrik-ilves-president-of-estonia-to-the-67th-session-of-the-united-nations-general-assembly-un-headquarters-new-york-september-2012/ and accessed June 2, 2019.

Chronology for Process Tracing

May 9, 2006: On Russian Victory Day, the red flags of the Soviet Union were flown at the Bronze Soldier while an Estonian tricolor flag was torn down. The police were unable to maintain public security if they removed the Soviet flags, so they left them where they were. This caused the Estonian people to demand the statue be removed lest it become a rallying point for Russian nationalism.[380]

January 10, 2007: Estonian government announces its plan to move the Bronze Soldier statue.[381]

January 2007: Russia's Upper House submits a resolution "demanding their Estonian parliamentary peers prevent the statue from being moved."[382]

Late January 2007: The Russian government summoned the Estonian Ambassador to express their dismay and to discourage moving the monument and human remains from the center of Tallinn to the cemetery.[383]

April 3, 2007: Sergei Ivanov, First Deputy Prime Minister (2007-2008) in Russia called on Russians to boycott Estonian goods and services in response to Estonia's plans: "Don't buy Estonian products [...], don't go to Estonia for vacations, go to Kaliningrad."[384]

Mid-April 2007: In the days prior to Phase I of the cyberattack, "Russian -language Internet discussion forums were abuzz with preparations for an online attack"[385] which points to a wide-ranging operational plan.

---

[380] "Estonia: Defense Minister Says Bronze Soldier Had To Go." *Radio Free Europe*, May 9, 2007.
[381] NATO Strategic Communications Centre of Excellence. "2007 cyberattacks on Estonia" Located at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf and accessed on November 24, 2019. p. 55.
[382] Schmidt, Andreas. "The Estonian Cyberattacks" in Jason Healey's *a Fierce Domain: Conflict in Cyberspace 1986-2012*. Washington DC: Cyber Conflict Studies Association, 2013. p. 175.
[383] Mardiste, David. "Russia to Estonia: Don't Move Our Statue." *Reuters*, January 25, 2007. https://www.reuters.com/article/us-estonia-russia-statue/russia-to-estonia-dont-move-our-statue-idUSL2378719620070125 and accessed on November 11, 2019.
[384] NATO Strategic Communications Centre of Excellence. "2007 cyberattacks on Estonia" Located at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf and accessed on November 24, 2019. p. 57.
[385] Evron, Gadi. "Battling Botnets and Online Mobs Estonia's Defense Efforts During the Internet War." *Georgetown Journal of International Affairs*; Winter/Spring 2008. p. 122

April 23, 2007: Estonia planned to highlight the online planning operations publicly, hoping that it would lead the European Union to admonish the plans and pressure the Kremlin to intervene. Unfortunately, Estonia was pressured from within the European Union to withhold the public warning and scolding due to an upcoming meeting between Russian President Putin and German Chancellor Merkel.[386]

April 26, 2007: Estonian government began initial preparations to relocate the Soviet-era "Bronze Statue" and soldier remains.

April 26, 2007 – April 29, 2007: Phase I of cyberattack launched against Estonia. Phase I consisted of relatively simple denial-of-service attacks and web defacement of high-profile and political sites including the President, the Parliament, police and major media outlets.[387] Online forums provided "step-by-step instructions so simple that any Internet user could follow, complete with a pre- selected list of targets"[388] for Phase I.

April 26, 2007 – April 27, 2007: The "Bronze Night" where rioting, fires and physical clashes with police occurred in Tallinn, Estonia.[389] "One man was killed, 153 people were injured, and some 800 arrests were made as the Russians resisted the removal of the bronze statue of a soldier."[390]

April 27, 2007, 3:40am: Emergency Parliament session called, government approves the immediate removal of the statue.[391] Later that day, the monument is removed and taken to an unknown location.[392]

---

[386] Evron, Gadi. "Battling Botnets and Online Mobs Estonia's Defense Efforts During the Internet War." *Georgetown Journal of International Affairs*; Winter/Spring 2008. p. 122

[387] Viira, Toomas. "Cyber Attacks Against Estonia - Overview and Conclusions." *Information Technology in Public Administration of Estonia - Yearbook 2007*. Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008. p. 71. The author of the article was the information security manager in the Estonian Informatics Centre in 2007. See also: NATO Strategic Communications Centre of Excellence. "2007 cyberattacks on Estonia" Located at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf and accessed on November 24, 2019. p. 55.

[388] Evron, Gadi. "Battling Botnets and Online Mobs Estonia's Defense Efforts During the Internet War." *Georgetown Journal of International Affairs*; Winter/Spring 2008. p. 123.

[389] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia. 2008

[390] "Tallinn tense after deadly riots." *BBC News*, April 28, 2007.

[391] Tapon, Francis. "The Bronze Soldier Explains Why Estonia Prepares For a Russian Cyberattack." *Forbes,* July 7, 2018. https:// www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-estonia-give-baltic-headaches/?sh=59f777da98c7 and accessed on November 14, 2019.

[392] "Tallinn tense after deadly riots." *BBC News*, April 28, 2007.

April 28, 2007: Estonian Ministry of Defense coordinates defense effort with CERT-EE, the Community Emergency Response Team for the Estonian .ee domain

April 28, 2007: Estonian Embassy in Moscow was surrounded by protestors demanding the resignations of the Government of Estonia and "subjected the Embassy officials inside the building to violence and vandalism."[393]

April 30, 2007 – May 19, 2007: Phase II of cyberattack. Phase II consisted of sophisticated, coordinated attacks using botnets and distributed denial-of-service. Targets included the data backbone network, government servers, two of the largest Estonia banks, Hansabank and SEB Eesti Uhisbank, and more extensive attacks on media outlets.[394] Phase II was significantly more technical than Phase I, both in the type of attack and the specific targets. While step-by-step directions for Phase I were widely publicized on the internet, no such guide existed for Phase II given the technical sophistication and funding required to carry out these operations.

During Phase II, Russia also suspended rail deliveries of raw materials and passenger service between some Estonian and Russian cities, but Russia claimed the suspension was not due to the political tension, but instead due to planned maintenance.[395]

April 30, 2007: Russian delegation visited Estonia and issued an official statement at the Embassy of the Russian Federation in Estonia that 'the government of Estonia must step down'[396]

May 2, 2007: Estonian Ambassador to Moscow physically attacked by protestors in Moscow while giving a press briefing.[397] Also, the European Commission urged Russia

---

[393] U.S. Senate. "Senate Resolution 187--CONDEMNING VIOLENCE IN ESTONIA AND ATTACKS ON ESTONIA'S EMBASSIES IN 2007 and EXPRESSING SOLIDARITY WITH THE GOVERNMENT AND THE PEOPLE OF ESTONIA." Congressional Record Volume 153, Number 72 (Thursday, May 3, 2007). Pages S5603-S5604. See also: Paet, Urmas. "Declaration of the Minister of Foreign Affairs of the Republic of Estonia." May 1, 2007. Located at: https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia and accessed on November 22, 2019.

[394] Viira, Toomas. "Cyber Attacks Against Estonia - Overview and Conclusions." *Information Technology in Public Administration of Estonia - Yearbook 2007*. Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008. p. 71. The author of the article was the information security manager in the Estonian Informatics Centre in 2007.

[395] "Russia Cuts Oil Product Exports via Estonia-source." *Reuters*, May 4, 2007.

[396] U.S. Senate. "Senate Resolution 187--CONDEMNING VIOLENCE IN ESTONIA AND ATTACKS ON ESTONIA'S EMBASSIES IN 2007 and EXPRESSING SOLIDARITY WITH THE GOVERNMENT AND THE PEOPLE OF ESTONIA." Congressional Record Volume 153, Number 72 (Thursday, May 3, 2007). Pages S5603-S5604.

[397] Republic of Estonia, Ministry of Foreign Affairs. "Estonian Ambassador to Moscow was attacked." May 2, 2007. Located at: https://vm.ee/en/news/estonian-ambassador-moscow-was-

to respect its obligations to the 1961 Vienna Convention on Diplomatic Relations and end the blockade of the Embassy of Estonia in Moscow. The Estonian Embassy in Moscow had been closed since April 27, 2007.[398]

May 9, 2007: The cyberattacks peak on this day and are unrelenting from 00:01 until midnight, 24:00. It is reported that, "You couldn't get information; you couldn't do your job. You couldn't reach the bank; you couldn't check the bus schedule."[399]

May 9th is also "Victory Day" in Russia, a celebrated Russian federal holiday. During a speech to Russian troops for the Victory Day celebration, President Putin remarked: "Those who attempt today to ...defile the monuments to war heroes are insulting their own people and spreading enmity and new distrust between countries and peoples."[400]

May 18, 2007-May 19, 2007, at midnight: The "cyberattacks abruptly and simultaneously cease."[401]

October 2007: NATO meeting of Allied Defense Ministers where they call for the development of an official NATO Cyber Defense policy. [402]

April 2-4, 2008: The Bucharest Summit marked the first time the Alliance formally discussed cyber issues within the summit framework. NATO adopted a Policy on Cyber Defense, and "are developing the structures and authorities to carry it out. Our Policy on Cyber Defense emphasizes the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyberattack. We look forward to continuing the development of NATO's cyber defense capabilities and

---

attacked and accessed on November 19, 2019.

[398] U.S. Senate. "Senate Resolution 187--CONDEMNING VIOLENCE IN ESTONIA AND ATTACKS ON ESTONIA'S EMBASSIES IN 2007 and EXPRESSING SOLIDARITY WITH THE GOVERNMENT AND THE PEOPLE OF ESTONIA." Congressional Record Volume 153, Number 72 (Thursday, May 3, 2007). Pages S5603-S5604.

[399] Mite, Valentinas. "Estonia: Attacks Seen as First Case of 'Cyberwar'." *Radio Free Europe/Radio Liberty*, May 30, 2007.

[400] Putin, Vladimir. "Speech at the Military Parade Celebrating the 62nd Anniversary of Victory in the Great Patriotic War," Kremlin transcripts, May 9, 2007. Located at: http://en.kremlin.ru/events/president/transcripts/24238 and accessed on November 21, 2019.

[401] NATO Strategic Communications Centre of Excellence. "2007 cyberattacks on Estonia" Located at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf and accessed on November 24, 2019. p. 55

[402] "NATO Opens New Center of Excellence on Cyber Defense." *NATO News*, May 14, 2008. Located at: https://www.nato.int/docu/update/2008/05-may/e0514a.html and accessed on January 3, 2019.

strengthening the linkages between NATO and national authorities.[403] The product of this policy is the creation of the NATO Cyber Center of Excellence.

May 14, 2008: NATO Cyber Center of Excellence opens in Tallinn, Estonia.[404] This Center serves as a multi-national hub of cyber expertise for NATO members and neighboring Nordic countries.

[403] "Bucharest Summit Declaration." *North Atlantic Treaty Organization*. April 3, 2008. Section 47. Located at: https://www.nato.int/cps/en/natolive/official_texts_8443.htm and accessed January 3, 2019.

[404] "NATO Opens New Center of Excellence on Cyber Defense." *NATO News*, May 14, 2008. Located at: https://www.nato.int/docu/update/2008/05-may/e0514a.html and accessed on January 3, 2019.

Structured Focused Questions

Targets

What were the targets of the cyberattack?

The attacks primarily consisted of denial-of-service (DoS), distributed-denial-of-service (DDoS) and website defacement. The DDoS attacks resulted in the "temporary degradation or loss of service on many commercial and government servers. While most of the attacks targeted non-critical services like public websites and e-mail, others concentrated on more vital targets, such as online banking and DNS.[405] Websites for the government, business community, banks, communications and media and political parties had to shut down when they were hit with the DDoS attacks. This meant that initially some digital government services were suspended, some digital banking was suspended, accessing some digitally-based local information and news was not possible, and several businesses were forced offline and unable to function. As the attack campaign continued, some victims were able to whitelist clients for access or put in other measures to allow some local IP access while preventing access from foreign IPs.

As noted above, May 9th is an important date for the Russians, when they commemorate Russia's Victory in Europe World War II with a celebration. It is also an important date for this cyberattack campaign because "on many sites the organizers called for an attack on that politically important date. The big attack wave anticipated for

[405] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia. 2008

May 9th started shortly after 11PM local time on May 8th, however, suggesting that these attackers were on Moscow time.[406]

The website defacement hit several sectors and consisted of replacing the original text with disinformation or pro-Russian propaganda and also included hacking the Estonian Prime Minister's site (who many believed to be the driving factor behind the relocation of the Bronze Soldier.)[407] The hackers who attacked the ruling Reform Party's website early on in the attack campaign left a bogus notice that the "Estonian prime minister and his government were asking forgiveness of Russians and promising to return the statue to its original site."[408] The targets of the cyberattacks broadly covered sectors of Estonian economic, government and society, all considered countervalue (including non-military government) targets, and did not appear to target counterforce targets.

Nature of Attack

What was the nature of the attack? How was the attack conducted?

As noted above, the cyberattacks largely consisted of DDoS and DoS attacks and website defacement, to include "modified attack tools, shared in forums by Russian (or Russian-language) hackers and, later, 'rented' distributed botnets nearly blocked

---

[406] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia. 2008. p. 3.
[407] Yasmann, Victor. "Russia: Monument Dispute with Estonia Gets Dirty." *Radio Free Europe*, May 4, 2007. Located at https://www.rferl.org/a/1076297.html and accessed on November 23, 2019.
[408] "The cyber raiders hitting Estonia." *BBC News*, May 17, 2007. Located at: http://news.bbc.co.uk/2/hi/europe/6665195.stm and accessed on November 23, 2019.

Estonia's access to the internet completely. The distributed nature of the botnet presented a more difficult challenge due to the need to defend against multiple attacking groups. "Two waves of attacks occurred — the second significantly more sophisticated than the first"[409] and "were unparalleled in size and variety compared to a country the size of Estonia.[410]

At first the Estonia perceived the internet attack as a nuisance, but quickly realized it was more than that when the targeting expanded to Internet addresses of servers supporting aspects of the telephone network, the credit card verification system, and the Domain Name System (DNS).[411] Over one million computers were involved in targeting servers in Estonia.[412] "Hansabank, the nation's largest bank, was staggered. Commerce and communications nationwide were being affected and the attacks did not stop. Estonia claimed that the ultimate controlling machines were in Russia another computer code involved have been written on Cyrillic alphabet keyboards."[413]

According to one cybersecurity company whose systems sees approximately 80% of the internet, it saw 128 unique DDoS attacks on Estonian websites in the first two

---

[409] NATO Strategic Communications Centre of Excellence. "2007 cyberattacks on Estonia" Located at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf and accessed on November 24, 2019. p. 53.

[410] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia. 2008

[411] DNS is the process to translate the human language-initiated web addresses into IP addresses. It is the system that allows people to type www.bu.edu and get a webpage instead of remembering to type 128.197.236.4 to read the BU homepage.

[412] Clarke, Richard and Robert Knake. Cyber War: The Next Threat to National Security and What To Do About It. New York: Harper Collins, 2010. p. 15.

[413] Clarke, Richard and Robert Knake. Cyber War: The Next Threat to National Security and What To Do About It. New York: Harper Collins, 2010. p. 15.

weeks of May using the company's unique threat analysis research infrastructure that examines internet traffic. Of these, 115 were Internet Control Message Protocol (ICMP) floods, 4 were Transmission Control Protocol (TCP) floods, and 9 were generic traffic floods. Attacks were not distributed uniformly, with some sites seeing more attacks than others in quantity; some attacks lasted under an hour while others persisted for hours and the largest recorded attacks were 40 gigabytes per second.[414] "The longest attacks themselves were over 10 and a half hours long sustained, dealing a truly crushing blow to the endpoints.[415]

Leadership as a Target, Potential Leadership Destabilization

Was leadership targeted?

Yes, the government websites of the Prime Minister were targeted; he was largely seen as a proponent of the plan to move the statue. The political website of the Reform Party was targeted and posting a fake disinformation message from the Prime Minister falsely apologizing for moving the statue.[416] It was left for the Estonian people to incorrectly believe their government was reversing course. The mail servers for Parliament were also targeted.[417] These cyberattacks on the leadership did not result in

[414] Nazario, Jose. "Estonian DDoS Attacks – A summary to Date." Published on Netscout Arbor, May 17, 2007.
[415] Nazario, Jose. "Estonian DDoS Attacks – A summary to Date." Published on Netscout Arbor, May 17, 2007.
[416] Ruus, Kertu. "Cyberwar I: Estonia Attacked from Russia." *European Affairs*, Volume 9, Issue 1, Winter/Spring 2008.
[417] Evron, Gadi. "Estonia 10 Years Later: Lessons learned from the World's First Internet War." Securityledger.com. April 28, 2017. Located at: https://securityledger.com/2017/04/estonia-10-years-later-lessonslearned-from-the-worlds-first-internet-war/

destabilizing the leadership; the attacks focused on the leadership were not sophisticated and did not impose large costs on the leadership.

Attribution

What was the understanding about attribution at the time of the attack? Did this change over time?

In the case of Estonia, "analysts determined the attacked traced back to 178 countries… [but that] served to muddy the obvious truth: The attacks were supported or encouraged by the Russian government and that to make the attacks stop, western decision makers needed to engage Moscow."[418] The Estonian government believed Russia was behind the attacks: "The European Union is under attack, as Russia is attacking Estonia."[419] The actions of the Russian delegation to Tallinn appeared to support this assertion. On April 30, a delegation from Russia's State Duma, the lower house of parliament, traveled to Tallinn to investigate the violent events surrounding the removal of the Bronze Soldier memorial. The delegation was headed by Nikolai Kovalyov who was then the head of the Duma Veterans Affairs Committee. While on the visit in Tallinn, Kovalyov called for the immediate resignation of the Estonian government.[420] Making this public statement following a crippling cyberattack campaign

[418] Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." *The Atlantic Council*, January 2012. p. 2-3.
[419] Paet, Urmas. "Declaration of the Minister of Foreign Affairs of the Republic of Estonia." May 1, 2007. Located at: https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia and accessed on November 22, 2019.
[420] Yasmann, Victor. "Russia: Monument Dispute with Estonia Gets Dirty." *Radio Free Europe*, May 4, 2007. Located at https://www.rferl.org/a/1076297.html and accessed on November 23,

that had been ongoing for over a week at that point and would continue for another two weeks, served to underscore the Kremlin's intention: at least to demoralize and punish Estonia for moving the statue and perhaps even as much as destabilize and undermine its control.[421] The Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyberattacks, noting:

> "When there are attacks coming from official IP addresses of Russian authorities and they are attacking not only our websites but our mobile phone network and our rescue service network, then it is already very dangerous."[422]

He also stated:

> "The attack is virtual, psychological and real – all at the same time. [...] IP addresses have helped to identify that the cyber terrorists' attacks against the Internet pages of Estonian government agencies and the Office of the President have originated from specific computers and persons in Russian government agencies, including the administration of the President of the Russian Federation."[423]

Paet was not the only official to publicly accuse Russia. Prime Minister Andrus Ansip charged:

> "the continuing cyberattacks from the servers of Russian state authorities, together with tearing the Estonian flag off our embassy and together with statements made by the delegates of the Russia Duma, calling for the change of government in Estonia, indicates that our sovereign state is under a heavy

---

2019.

[421] A smart strategy is to undermine the leadership of one's enemies and cause them domestic strife which then weakens them overall and leaves the population susceptible to outside influence. A leading Russian cyber-strategist, Sergei Rastorguev, wrote about population manipulation and how to goal in information warfare is to get the enemy to disarm themselves instead of an opponent causing it to occur. The strategy is quoted in Gadi Evron's "A Russian Strategist's Take on Information Warfare." Darkreading.com, March 26, 2010.

[422] Bright, Arthur. "Estonia Accuses Russia of 'cyberattack'." *CSMonitor,* May 17, 2007.

[423] Paet, Urmas. "Declaration of the Minister of Foreign Affairs of the Republic of Estonia." May 1, 2007. Located at: https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia and accessed on November 22, 2019.

attack."[424]

The President of the European Parliament at the time, Hans-Gert Pottering, noted that "it is usual in Europe to demand the resignation of a democratically elected government of the neighboring country. It is unthinkable in Europe to disregard the Vienna Convention on the protection of the diplomatic representations."[425]

In additional to the technical data and obvious heightened tensions surrounding the relocation issue, there are a number of real-world political and economic actions from the Russian government and Russian government figures that occurred in parallel to the cyberattacks and contributed to the assessment of the attribution of the attack. With these supporting statements, the cyberattack against Estonia can be ranked on Healey's Spectrum of State Responsibility between 4, State-Encouraged, and 9, State-executed.[426] Looking at the public statements from Estonian leadership during this timeframe, it is clear that they believed attribution was between 5, State-shaped and 9, State-executed. While Sharp's Known Coercer + Known Demand model denotes this cyberattack as "less certain" and therefore "indeterminate" on whether this was a case cyber coercion, the Estonia leadership was certain, supported by the real world actions and the technical data

[424] Anderson, Nate. "Massive DDoS attacks target Estonia; Russia accused." *ArsTechnica*, May 14, 2007. Located at: https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/ and accessed on November 2, 2019.
[425] Anderson, Nate. "Massive DDoS attacks target Estonia; Russia accused." *ArsTechnica*, May 14, 2007. Located at: https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/ and accessed on November 2, 2019. See also: Paet, Urmas. "Declaration of the Minister of Foreign Affairs of the Republic of Estonia." May 1, 2007. Located at: https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia and accessed on November 22, 2019.
[426] Healey's Spectrum of State Responsibility was created long after the 2007 Estonia attacks, but it is a useful tool to employ in assessing the cyberattack.

provides a level of confidence in Estonia's attribution.

"Clear political signatures were even detected in the malicious network traffic. All told, it is clear that the cyberattacks were linked with the overall political conflict between Estonia and Russia."[427] To aid in the attribution question, one must look at these real-world activities, specifically the economic sanctions and Russia's decision to ignore its treaty obligations with Estonia. "Russia suspended certain rail deliveries of raw materials and passenger service between Tallinn and St. Petersburg" for a period of time during the attack campaign.[428]

Further, the Estonian government notified Russian officials that it traced some of the command and control of the campaign back to Russia, to which Russia responded by excusing the behavior and noted that patriotic Russians may have acted independently. Russia declined Estonia's formal diplomatic request to pursue the matter through its internal services and law enforcement or acting to prohibit further attacks originating from Russian control, dodging a treaty obligation with Estonia. The most likely conclusion for this behavior is that these actions served Russia's interests.[429]

At an event marking the ten years since the 2007 cyberattacks, speaking on the attribution of the attack by Russia, the President of Estonia noted: "Certainly the fact that

---

[427] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia. 2008

[428] Anderson, Nate. "Massive DDoS attacks target Estonia; Russia accused." *ArsTechnica*, May 14, 2007. Located at: https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/ and accessed on November 2, 2019. Russia claimed that this closure was part of regularly scheduled maintenance.

[429] Clarke, Richard and Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins, 2010. p. 15.

a year later they use the same methods [in the cyberattacks against Georgia] and combined them with kinetic attacks, they saw it was a success [in Estonia.]"[430] He also noted that when Georgia was the victim of the same methods the following year, that Estonia "set up mirror sites to help them so they… could access more important sites, they would re-route to us [Estonia]."[431] In a separate interview, Ilves noted that this type of cyberattack had never been done until Estonia and then it happens again a year later,

> moreover corroborating our initial beliefs that it was the Russians, same methodology, but then, combining that with more than just taking down servers, but also taking the servers down in conjunction with actual physical military attacks. It's just a new level that they applied to Georgia.[432]

Audience Costs

What were the audience costs? What were the audience costs over time?

The domestic audience costs for Estonia were high, both for sustaining the attack and for responding to the aggressor. Having already suffered significant strife, extensive protests and some violent rioting prior to the actual relocation of the Bronze Soldier statue, having its government, media, business and banking systems paralyzed was a significant event. It made an even greater impact on society than one might assume since the country was so heavily reliant on its digital infrastructure for daily life, much more so that the United States or most European countries in 2007. To complicate matters, the

---

[430] Interview with Toomas Hendrik Ilves, President of Estonia, 2007 – 2016. "10 Years of Cyber Estonia: What will the Next Decade Bring?" *Center for Strategic and International Studies*, November 6, 2017.
[431]Interview with Toomas Hendrik Ilves, President of Estonia, 2007 – 2016. "10 Years of Cyber Estonia: What will the Next Decade Bring?" *Center for Strategic and International Studies*, November 6, 2017.
[432] Gilmore, Jim. "Interview with Toomas Henrik Ilves." *Frontline*, June 23, 2017.

domestic schism on feelings toward Russia in the post-1991 independence declaration, was another factor of domestic audience costs. The relatively recent reminder of life under Soviet control served as a reminder of the importance of defending itself against Russian aggression in all forms. If Estonia acquiesced to Russia on the Bronze Soldier statue, especially after such a broad and public cyber coercive action, the audience costs faced by the President would have been considerable and potentially career-ending. "The attack could have resulted in a weakening of Estonian citizens' trust in the government's ability to defend the country against unconventional attacks, but the quick response of the government, together with support from NATO and many nations in ensuring recovery, prevented widespread public distrust."[433]

The fight over the statue might be a situation where the Estonians were not willing to budge regardless of any Russian threat or action, however, the public nature of the cyber coercion strategy that Russia chose resulted in audience costs for the leadership that made it impossible for Estonia to acquiesce. If the Russians had engaged in a less public cyberattack or targeted the leadership in particular to gain personal information that could be used to coerce them personally on this issue, then there is a greater chance they might be successful. However, given the history of Estonia and Russia,

[433] NATO Strategic Communications Centre of Excellence. "2007 cyberattacks on Estonia" Located at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf and accessed on November 24, 2019. p. 53.

Financial Costs

What were the financial costs? What were the financial costs over time?

The total financial cost of the 22 days of cyberattacks is hard to measure, but likely in the billions of Euros. One institution, Estonia's Hansabank, reports that it alone lost at least $1million due to the attacks.[434] "Estonia faced lost productivity, opportunity cost, remediation, and the acquisition of alternative web hosting at emergency rates estimated to be in the billions of Euro."[435] The 2007 cyberattacks did not leave lasting or permanent damage, but certainly disrupted finance, media, government and a whole host of businesses for the time period of the attack campaign.

Pressure on Leadership

What was the pressure on leadership during the cyber crisis?

With an inability to carryout daily digital activities including banking and accessing the news, there was a concern about what additional attacks might occur and for how long Estonia would experience digital paralysis. Due to the public nature of the cyberattacks, there was immense pressure on leadership during this crisis. Beyond the obvious pressure from the cyberattack, since Estonia was a leading digital-based country in Europe, there was increased pressure to solve the issue swiftly so as not to lose the population's trust in relying on digital services. If the Russians could disrupt and

---

[434] Mite, Valentinas. "Estonia: Attacks Seen as First Case of "Cyberwar." *Radio Free Europe*, May 30, 2007.

[435] NATO Strategic Communications Centre of Excellence. "2007 cyberattacks on Estonia" Located at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf and accessed on November 24, 2019. p. 53.

undermine Estonian reliance on its digital infrastructure, it would also serve to undercut the government's digital strategy and, in 2007, undermine the decade-long government strategy to make Estonia a leading technologically advanced country. That is, if a Russian cyberattack could significantly disrupt daily Estonian life, long-term, the Estonian people may prefer to be less digitally-dependent in the future.

George's seven conditions as structured focused questions:

Clarity of the Objective

What was the victim's understanding of the clarity of the objective?

In this case study, the victim was not aware initially what was happening, as attested to by former President Ilves. Once they realized this was a coordinated cyberattack, the leadership clearly believed that the attack was launched due to the controversial relocation of the Bronze Soldier statue and associated human remains. As described above, upon recognition that it was a coordinated attack, and in conjunction with the statements from the Russian Duma, the leadership in Estonia believed the attack originated from Russia and that the demand was not to move the statue and remains, as Russia had been requesting since at least January of that year.[436]

[436] Mardiste, David. "Russia to Estonia: Don't Move Our Statue." *Reuters*, January 25, 2007. https://www.reuters.com/article/us-estonia-russia-statue/russia-to-estonia-dont-move-our-statue-idUSL2378719620070125 and accessed on November 11, 2019.

Strength of Motivation of Coercer

What was strength of motivation of the coercing power?

The coercing power, Russia, was particularly strongly motivated because it interpreted the relocation of the Bronze Soldier statue as an affront to the history, valor and memory of the Red Army. When viewed through the lens that Russia celebrates May 9th, Victory Day over the Nazis, with a federal holiday and, in recent decades, large popular celebrations, it is easier to understand why the relocation of one statue caused such a high level of conflict. Russia felt so strongly about the possibility of moving the statue that it formally requested a meeting with the Estonian Ambassador in Moscow to express its anger, diplomatically. To the Russians, this was not simply relocating a statue; it was

Asymmetry of Motivation

What was the asymmetry of motivation between the adversaries?

There did not appear to be asymmetry of motivation between the adversaries. The Russians sought to punish the Estonia's for the perceived disrespect of the Red Army and the Estonians were steadfast in their determination to move the Bronze Soldier statue. The fact that an emergency session of Parliament was called at 3:40am to vote to move it immediately supports the assertion that the Estonians were just as motivated to move the monument as the Russians were to try to coerce them to change their decision and not to move it. The Estonians also pursued a significant defense, including calling for additional support from NATO and cyber experts in the region, to defend itself against Russian

cyber aggression.

Estonia had significant domestic and patriotic investment in moving the Bronze Soldier statue. "Over the past few years [preceding 2007] the statue had become a focal point of tension between pro-Kremlin and Estonian nationalist movements."[437] The comprehensive assault on its digital infrastructure that touched critical economic sectors was a strategy of coercion that back-fired on the aggressor. At first, Estonia employed a combination strategy, first doing nothing in response and then defending and mitigating what they could with whitelisting domestic addresses only. This meant that only internet traffic originating from inside the country could get through. The point was to eliminate all the external incoming traffic requests. Estonia continued to proceed with moving the Bronze Soldier statue and the associated remains, while also continuing to defend itself, reconstitute where possible and mitigate the attacks, if possible. "To prevent further attacks [at one point], Estonia had to close off parts of its network to computer users outside the country, isolating itself from the rest of the Internet."[438] Estonia did not waver in its determination and the extensive digital assault forced it to defend itself. Whereas a different targeting approach, perhaps one more limited, may not have resulted in defensive behavior to the extent seen in 2007 and the follow-on cooperation with NATO in 2007-2008. In the long-term, Estonia engaged in mounting a heavy defense and continued to improve on its modern digital system to ensure that it would be extremely

[437] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia. 2008

[438] Mite, Valentinas. "Estonia: Attacks Seen as First Case of "Cyberwar." *Radio Free Europe*, May 30, 2007.

difficult for any aggressor to hack in the future. For Estonia, cyber coercion resulted a stronger defense and increased cooperation with NATO on cyber matters.

The cyberattack against Estonia was not considered successful long-term for Russia because not only did Estonia increase its cyber defenses domestically, NATO realized the severity of the Russian provocation via cyberattack as a threat and created the NATO Cyber Centre of Excellence, and NATO chose to headquarter it in Tallinn, Estonia. The 2007 Russian cyberattack against Estonia resulted in the NATO community coalescing around the view that the cyber threat was real, that it was significant, that it required dedicated attention and funding, and an overarching strategy and they acted accordingly. This was a less-than-ideal scenario for the Russian coercion strategy. As stated before, similar to diplomatic coercion, cyber coercion is a tricky dance requiring a coercer to push, but not too far and to choose the correct levers to exercise power because mistakes can backfire, and backfire it did for the Russian strategy in meeting its stated goal. However, Russia did benefit from this activity because it was able to see what actions it could take in cyberspace that did not result in a NATO action against Russia, and it was able to learn from its operations and adapt best practices and lessons learned when it conducted similar attacks on Georgia the following year and, later, in Ukraine.

"Estonia 2007 was the first cyberattack in history that affected a country nation-wide," said Helen Popp, counselor for cyber issues at the Estonian Embassy in Washington, D.C. The increased "awareness, understanding, resilience and defense capability" stemming from that attack in Estonia and inside NATO, she said, "has been

immense."[439] At the United Nations Security Council in 2019, Estonia brought up cyber threats for the first time in that forum. According to the current President of Estonia, Kersti Kaljulaid:

> "When we finally had a really good conference on the 8th of May in the UN Security Council, somebody quipped that it was probably a small step for Estonia but a big step for the world and I have to say that it does not exactly sound modest if I confirm but we felt a little bit this way. Our point has been proven." …"Our goal [in going to the UN Security Council] was to start creating the new normal; that if a country comes under cyberattack, then they will have at the Security Council a place to report about it, complain about it, and ask other countries to react, take positions, and maybe one day also take action. …We still do not have a clear understanding of how we are able to protect our sovereignty [in cyber].[440]

Victim Understanding of Urgency

What was the victim's understanding of the coercer's sense of urgency?

Estonia was acutely aware of Russia's sense of urgency that the Bronze Soldier statue and related soldier's remains not be moved. This determination is based on the public statements of Estonian government officials and Russian government officials during the conflict, along with the violent riots and protests in Tallin and Moscow immediately preceding the relocation.

---

[439] Tamkin, Emily. "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy*, April 27, 2017.
[440] President of Estonia, Kersti Kaljulaid, remarks presented at "Deciding on the Rules of the Road for Cyberspace: The Who, What, Where, When, How" at the Institute of International Cyber Stability, June 9. 2020.

Adequate Domestic and International Support

Is there adequate domestic and international support for the victim and the coercer?

There was adequate domestic support for both the victim and the coercer in their respective polities. In Estonia, the level of domestic support was clouded by the violent protests and clashes between ethnic Russians and ethnic Estonians living in Estonia, but especially given the history of Soviet rule, fighting Russian aggression was very important to the domestic audience. As for international support, the Estonian defense minister noted that, at the time, "NATO does not define cyberattacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defense, will not automatically be extended to the attacked country."[441] The international support for the victim was demonstrated by NATO's voluntary assistance, in lieu of Article 5 activation, in pursuit and defense in the immediate term, and of course by the longer-term NATO investment in Tallinn as the Cyber Centre of Excellence, created in 2008. As noted earlier, the U.S. Senate made a resolution expressing solidarity with Estonia in the face of these cyberattacks;[442] and the European Parliament expressed support and solidarity with Estonia while also condemning Russian escalatory actions and rhetoric.[443]

---

[441] Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian.* May 16, 2007.
[442] U.S. Senate. "Senate Resolution 187--CONDEMNING VIOLENCE IN ESTONIA AND ATTACKS ON ESTONIA'S EMBASSIES IN 2007 and EXPRESSING SOLIDARITY WITH THE GOVERNMENT AND THE PEOPLE OF ESTONIA." Congressional Record Volume 153, Number 72 (Thursday, May 3, 2007). Pages S5603-S5604.
[443] "European Parliament resolution of 24 May 2007 on Estonia." European Parliament, Document RC-B6-0205/2007, Texts Adopted, Strasbourg, France.

Estonia was able to use this unfortunate experience to bolster its relationship with other NATO members, take advantage of the opportunity to lead and teach NATO members about cybersecurity and how to best defend itself against cyber aggression, and build a stronger cyber-focused coalition. In the absence of such a massive attack, it may have been difficult to coalesce NATO member's opinions around cyber defense as an extremely important topic worthy of investment, let alone secure investment in a NATO Cyber Centre in Tallinn.

As for the aggressor, Russia did not have international support for its cyber coercive efforts, but it did not appear that international support, in this case, was important nor necessary for Russia to conduct the offensive cyber actions. Russia enjoyed domestic support on this topic, especially since framing the issue as one that was blasphemous to Russian history. That being said, during the 2007 timeframe, Russia was rated as "not free" as a measure of democracy for political rights and civil liberties, according to Freedom House.[444] Therefore, while Russia did have domestic support, the level of domestic support may not be as important for this aggressor as it might be for a free democracy.

Fear of Unacceptable Escalation

What is the opponent's (victim's) fear of unacceptable escalation?

Estonia appeared to have a high tolerance for escalation in this situation. "Estonia

[444] "Russia." Freedom House, 2007. Located at: https://freedomhouse.org/report/freedom-world/2007/russia and accessed on December 18, 2019.

did not consider the event as an armed attack and thus refrained from requesting NATO's support under Art. 5 of the NATO Treaty."[445] When this cyberattack occurred, the Estonian defense minister, Jaak Aaviksoo, said: "Not a single NATO defense minister would define a cyberattack as a clear military action at present. However, this matter needs to be resolved in the near future."[446] The then-President of Estonia, Toomas Henrik Ilves, has provided testimony to the U.S. Senate and has been interviewed a number of times about the 2007 cyberattack; he consistently characterizes the cyberattack as the first time "a nation-state had been targeted using digital means for political objectives"[447] and consistently invokes von Clausewitz's principle that the cyberattacks were clearly a continuation of policy by other means. In none of his written testimony nor interviews does he ever mention nor allude to a fear that, in 2007, they were concerned about physical escalation of this tension beyond the initial protests and blockade of their embassy in Moscow. He has, however, remarked repeatedly that Russia learned from its experience in Estonia and, the following year, complemented its cyberattacks against Georgia with kinetic strikes.

According to the statements from the Estonian government leadership, they did not

---

[445] Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security." *International Journal of Cyber Warfare and Terrorism*, 1(1), 24-34, January-March 2011. p 25.
[446] Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian.* May 16, 2007.
[447] [447] Ilves, Toomas. "Prepared Testimony and Statement for the Record of Toomas Hendrik Ilves, President of Estonia 2006-2016 At the Hearing on 'The Modus Operandi and Toolbox of Russia and Other Autocracies for Undermining Democracies Throughout the World.' Before the Senate Judiciary Subcommittee on Crime and Terrorism March 15, 2017. Located at: https://www.judiciary.senate.gov/imo/media/doc/03-15-17%20Ilves%20Testimony.pdf and accessed on June 10, 2019.

anticipate a physical world or kinetic action to accompany the cyber actions and escalate the conflict to an unacceptable level in 2007. An unacceptable level could be defined as an armed attack to complement the cyberattack, a hybrid warfare strategy, like Georgia experienced the following year.

Having its digital systems incapacitated by DDoS and DoS attacks for 22 days along with website defacement with disinformation, led Estonia to defend itself in the long-term instead of capitulating. If Russia chose counterforce targets instead of countervalue targets or chose a different type of attack with more lasting or permanent consequences, such as stealing and leaking sensitive data, or threatened to conduct operations in the physical world, Estonia's calculation for its unacceptable escalation may have been different.

Clarity on Terms for Settlement

What is the clarity concerning precise terms of the settlement of a crisis for the victim and the coercer?

Estonia clearly understood that the terms of the coercion settlement was to not relocate the Bronze Soldier statue nor disrupt the human remains and maintain the current site for the monument in downtown Tallinn.

Conclusion

The attack on Estonia was a watershed moment for cyber statecraft. It was an expansive attack, focused heavily on civilian infrastructure and systems needed to support daily life in Estonia. The typical Estonian citizen was affected by this cyberattack by an inability to access media, news, banking systems or a variety of other services that relied on the backbone that was attacked. This of course was in addition to the government sites that were attacked, but most people do not access their government services on a daily basis like they do with news or banking. This meant that this cyberattack affected the Estonians in a much more expansive and personal way, incurring higher audience costs, than if it had been solely targeted on military and government networks that would not have consequences for most of the population on a daily basis.

The nature of the attack, the duration, and choice of both commercial and government targets contributed to the significant audience costs faced by the Estonian leadership. Further, the financial costs borne by private industry and the government while business was frozen and the government scrambled to defend its infrastructure put high pressure on the Estonian leadership to resolve the issue. The impact of these additional variables on the outcome will be thoroughly discussed in the following chapter.

Reexamining this influential case and subsequent actions of the Russians, the former President of Estonia notes:

> "If you look at the situation today [2017], to say that they [Russians] were tactically brilliant and must be congratulating themselves on all they managed to do [via offensive cyber actions in the last ten years], tactically great. Great job.

> Strategically you have managed to alienate… Germany is now really angry at Russia, Emanuel Macron [after being a victim to cyberattacks]…now has a very different take on Russia. I think what they have done, is a failure. You have managed to alienate many of the biggest countries in the West."[448]

Ilves noted, in 2017, that one solution to fighting cyberattacks in a world of self-help is to create a "community or league of democracies, …a new form of defense organization, a non-geographical but strict criteria-based organization to defend democracies…."[449] In the immediate aftermath of the 2007 attack, NATO was energized to create a Cyber Centre of Excellence and headquarter it in Tallinn, centering the cyber expertise in the capital city of the Russian victim. Estonia built cyber resilience for themselves, extending this knowledge and partnering with NATO to ensure best practices throughout the NATO alliance. Further, Estonia worked with its non-NATO Nordic neighbors to ensure they, too, managed their cyber risk and shared best practices. This defense collaboration served as a balancing function against Russia in cyber statecraft. Estonia worked to shore up not only its defenses, but those of NATO and Nordic countries bordering Russia which are some of the most likely potential future victims of Russian cyber statecraft. Not only did Russia's cyber actions against Estonia fail to achieve their goal, they resulted in significantly increased cyber defenses not only of the

---

[448]Interview with Toomas Hendrik Ilves, President of Estonia, 2007 – 2016. "10 Years of Cyber Estonia: What will the Next Decade Bring?" Center for Strategic and International Studies, November 6, 2017.

[449] Ilves, Toomas. "Prepared Testimony and Statement for the Record of Toomas Hendrik Ilves, President of Estonia 2006-2016 At the Hearing on 'The Modus Operandi and Toolbox of Russia and Other Autocracies for Undermining Democracies Throughout the World.' Before the Senate Judiciary Subcommittee on Crime and Terrorism March 15, 2017. Located at: https://www.judiciary.senate.gov/imo/media/doc/03-15-17%20Ilves%20Testimony.pdf and accessed on June 10, 2019.

initial intended victim, Estonia, but of the entire region.

That being said, this cyber coercive conflict provided Russia with an ability to exercise and test their capabilities, learn and adapt for future conflicts, including Georgia the following year and, later, Ukraine. Further, since this was Russia's first use of extensive cyberattacks against a state's soft, countervalue targets, they learned that the extent of disruption they caused in Estonia did not result in an immediate NATO defense declaration. So, while the NATO CCDCOE in Tallinn was created, invested in and increased cyber knowledge-sharing and, eventually, improved cyber defenses, Russia was able to significantly disrupt daily life in Estonia without provoking a NATO collective defense declaration.

From a policy perspective, this case study provides several opportunities for future work that will be elaborated on in detail in Chapter 7. Policy research stemming from this case study includes disincentives for targeting commercial targets, cyberattack disclosure requirements, international agreements for enhanced cyber defense and deterrence, and looking at tiered agreements to account for the states that, thus far, refuse to sign onto international agreements on behavior and norms in cyberspace.

CHAPTER 6: HYPOTHESIS TESTING

This chapter has two goals. First, to test the multiple hypotheses using process-tracing to examine the relationship between the values of the independent variables and the decisions victims make in responding to cyber coercion, the dependent variables, over three temporal values. Second, this research uses the data assembled from the structured focused questions to perform a comparative analysis. It examines the conditional influence of a set of variables on why cyber coercion may achieve a degree to effectiveness in changing a victim's behavior over time. Looking at a pair of most-similar cases that share significant background factors allows me to highlight which independent variables impacted the victims behavior to result in these divergent outcomes. This chapter also provides a better means of analyzing these cyber coercive dyads. Namely, instead of the binary winners/losers narrative used in the literature, this research looks at a spectrum of victim responses in determining how effective and efficient the coercion was in achieving the goal, or part of the goal. Further, it shows how the accepted narrative is incorrect for each dyad and provides a new understanding of these case studies when looking at the interactions and decision-making over time. These two methods, used in tandem, demonstrate and describe in detail the factors that were and were not present in each case study and also to show how and why these factors contributed to the causal influence that resulted in each outcome. Lastly, this chapter shows that a Utilitarian approach to cyber coercion has a place in the literature, and in practice, that neither the first wave pessimists nor second wave optimists recognized. Although cyber coercion is unlikely to cause catastrophic death, a lack of body counts

does not render it useless and is not necessary in order for it to be effective for coercive diplomacy.

The data reflects that the main factors in these particular cyber coercive dyads that impacted the divergent victim decision making are asymmetry of motivation, opponents fear of unacceptable escalation, audience costs, financial costs, the choice of target, and targeting of leadership that led to leadership destabilization. These variables contributed to the increase or decrease of the likelihood of a victim changing its behavior.
As noted earlier, the exogenous factor in the North Korea vs. Sony case study of a subsequent physical threat contributed to Sony's compellence and, in conjunction with the cyber coercion, caused the secondary deterrence effects as well.

"Throughout all of his writings George emphasized the limitations of abstract deductive theory and argued that both explanatory theory and policy relevant theory required conditional generalizations that were context dependent and informed by history."[450] He also cautioned that the choice of a particular coercive strategy depends on the individual context of the crisis event, so there is no widely generalizable theory when it comes to coercive diplomacy. Instead, there are factors to identify that can lend themselves to increasing or reducing the likelihood of coercion being effective, and with the addition of the extended variables tested in this research, this idea can be applied to cyber coercion.

[450] Levy, Jack. "Deterrence and Coercive Diplomacy: The Contributions of Alexander George." *Political Psychology*, Vol. 29, No. 4, 2008 537-552. p. 538

Case of North Korea vs. Sony

Below is a table showing the changes of the independent variables across three temporal values for the Sony Pictures Entertainment-North Korea case study. The dependent variable can be shown as an escalation spectrum of options over time. This dependent variable escalation spectrum is used to examine each dyad of cyber coercion over three temporal values. For the North Korea-Sony Pictures Entertainment dyad these are:

Time 1 – November 21, 2014 – December 1, 2014: the initial period of attack up to the first data release - Sony Pictures Entertainment was internally chaotic given the inability to access its systems and did not respond to the GOP threat.

Time 2 – December 2, 2014 – December 21, 2014: Sony capitulated by cancelling the movie and then changed that decision and partially capitulated by lowering distribution of the film and releasing it via video on demand. SPE also faced ongoing, expensive technology failures and suffered increased audience costs.

Time 3 – December 22, 2014 – February 2016: Sony and other studios cancelled future films featuring North Korea, an SPE leader was forced to step down from her job and said that she was fired due to the consequences from the cyberattack.[451]

[451] McNary, Dave. "Amy Pascal Talks Getting 'Fired,' Sony Hack and Angelina Jolie Emails in Candid Interview." *Variety,* February 11, 2015.

Table 7:

NORTH KOREA vs. SONY PICTURES ENTERTAINMENT	
T0	The buildup to the conflict was Sony's announcement of a parody film about killing the North Korean leader and North Korea publicly demanded the film not be released
T1 Initial attack and first round of data published	*Present IVs:* Targets: Countervalue Nature: Sophisticated, extensive IT damage, confusion for victim Attribution; Audience costs; Financial costs; Pressure on leadership; Clear objective; Strong coercer motivation; Asymmetry of motivation; Sense of urgency; Adequate support; Clear and precise terms *Not Present IVs:* No leadership as a target, no potential destabilization, minor audience costs at this time; No opponent fear of unacceptable escalation due in part to the internal chaos and focus on keeping the business running.
	Present DV: DV: status quo ante: no action Result: Victim does not change behavior nor acquiesce to demand
T2 Secondary phase including threat of physical violence and ongoing ramifications from attack; rounds two through nine of data published	*Present IVs:* Targets: Countervalue Nature: Sophisticated, extensive IT damage, exogenous threat of physical violence Leadership as a target, potential destabilization; Attribution; Audience costs; Financial costs; Pressure on leadership; Clear objective; Strong coercer motivation; Asymmetry of motivation; Sense of urgency; Adequate support; Opponent fear of unacceptable escalation; Clear and precise terms *Not Present IVs:* None
	Present DV: DV: Initial complete compellence, then a reversal and partial compellence – victim behavior change Result: Victim announces it will acquiesce to demand, then reverses this acquiescence and plans to release it.

Table 7 continued:

T3 Post attack period: December 22, 2014 - February 2016	*Present IVs:* Targets: Countervalue Nature: post-attack Leadership as a target, actual destabilization; Attribution; Audience costs; Financial costs; Pressure on leadership; Clear objective; Strong coercer motivation; Asymmetry of motivation; Sense of urgency; Adequate support; Opponent fear of unacceptable escalation; Clear and precise terms *Not Present IVs:* None, while the cyberattack is no longer occurring, Sony Pictures deals with the fallout
	Present DV: DV: continued partial compellence, longer-term compellence and deterrence of pursuing other North Korean-related projects Result: Victim released film to small independent theatres and video-on-demand, a significantly lower audience than was originally intended for the film. Leadership executive fired as a consequence of the cyberattack.

The conventional wisdom is that the North Korea hack of Sony Pictures Entertainment was a failure because the movie eventually was released. This is not true. As this research has shown, tracing the process of the decision-making reveals that Sony Pictures pared down the promotion and release of the film, which reduced its expected revenue. As the cyberattack and publication of the stolen data ensued, each decision that Sony Pictures made to cancel the planned promotion and restrict the release of the film served North Korea's interest. Further, Sony Pictures fired one of their executives as a direct consequence of this cyberattack, including the reputational costs it incurred, and had to pay millions in remediation costs to get its network up and running again.

Hypothesis 1: George's seven conditions that favor coercive success (Clarity of the objective, Strength of Motivation, Asymmetry of Motivation, Sense of Urgency, Adequate Domestic and International Support, Opponent's Fear of Unacceptable Escalation, and Clarity Concerning Precise Terms of the Settlement of a Crisis) will fully explain the outcome.

Status: Reject

Explanation:

While George's seven conditions that favor coercive diplomacy cover a breadth and depth of cases in the purely diplomatic realm, cyber statecraft and by extension cyber coercive acts require additional variables to truly capture all the factors that can affect the outcome of a cyber coercive conflict. For example, a prominent aspect of a cyberattack is its nature: namely, whether it is amateurish or sophisticated. Other components to the nature of the cyberattack include the duration (e.g. sophisticated attacks that last weeks or months will be viewed differently from amateur attacks that are a one-time occurrence) and the strategic choices made during the conduct of the attack (e.g. the adaptations the aggressor makes to continue the attack or leveraging the cyber access to ratchet up pressure by gradually destroying systems over time or by slowly disclosing sensitive stolen information.) The nature of the cyberattack is a factor that the victim uses to determine its response and how seriously it ought to take a threat. For the cyberattack against Sony, it was a sophisticated attack that paralyzed the company's technical systems for weeks and slowly intensified pressure by releasing batches of sensitive data over weeks. The components of the nature of an attack are necessary factors to include in

determining what variables contribute to the likelihood of a victim changing its behavior.

Further, as this case study has shown, leadership as a target, the potential for leadership destabilization, and the pressure on leadership are factors that apply to both cyber coercion and coercive diplomacy. While George briefly touches on the idea of strong leadership, he does not explicitly denote leadership as a target and does not address the ramifications of targeting leadership for destabilization. While that may not be a practice often seen in traditional coercive diplomacy, it is most definitely a strategic option for an aggressor in cyber coercion and ought to be accounted for as a factor that affects the outcome. In the example of the Sony Pictures attack, the focus on targeting leadership communications, especially salacious ones, and strategically disclosing these communications in a slow and steady manner to increase internal pressure was clearly successful in one aspect, getting an executive fired.

Finally, audience costs and financial costs are also key variables affecting outcomes in cyber statecraft in a different way than economic sanctions, blockades and embargoes do in traditional coercive diplomacy. In the case of Sony Pictures, a commercial company, it is a soft target with fewer defense capabilities than a nation state. It faced extremely high audience costs as its internal documents were disclosed, with each round of publication containing a range of juicy gossip to substantial security and business information. The media was so hyper focused on analyzing and publishing stories on the information that the Sony Pictures attorney threatened legal action if media outlets continued to do so. A Sony Pictures executive lost her job as a direct consequence of the cyberattack and associated audience costs.

Finally, the financial costs levied against a commercial entity are different than a nation state target, especially over time. A commercial entity has stockholders and a board to respond to, so there are limits to the financial costs they can incur before the pressure to acquiesce to a demand is "cheaper" financially and/or reputationally. Further, private industry also has the option of insurance and passing the costs of the cyberattack on to the insurance industry so that insurance pays for the actual cost of the attacks. Additionally, leaders have the self-interest of keeping their job, so if the financial and audience costs incurred jeopardize their position, they may be pressured to acquiesce sooner in order to ensure their job security. These additional factors are essential to include when assessing the variables that affect cyber coercive outcomes.

While George hypothesizes that his seven factors are sufficient in investigating what favors the success or failure of coercive diplomacy, this research argues that these seven factors are insufficient to apply to the effectiveness of cyber coercion. Instead, additional factors must also be considered when looking at what factors favor cyber coercive outcomes and that is due, in part, to the nature of cyber coercion and the aggressor's strategic choices. That is, having access to internal files and private communications and driving up audience costs by revealing this information slowly and publicly, especially given the scale possible in cyber coercion, is distinctly different from the practice of diplomatic coercion. Additionally, the ability to destroy an expensive network on which an entity is highly-dependent, without engaging in a kinetic action, is also something that is particular to the cyber realm. An aggressor can drive up financial costs exponentially simply by executing code and taking advantage of a victim's

vulnerabilities. Therefore, these additional factors ought to be included when discussing the variables that favor cyber coercion.

Hypothesis 2: All other variables being equal, the greater the financial and/or audience costs faced by a victim where there is asymmetric motivation combined with a potential for leadership destabilization, the more likely the victim is to acquiesce to the demands of the aggressor over time.

Status: Partial acceptance with modification

Explanation:

For Sony Pictures, there were high audience costs, the ramifications from the rounds of publications of internal data, and the financial costs certainly did put pressure on the company to acquiesce. With North Korea calling this film's release an "act of war" it was clear that there was an asymmetric motivation, although Sony Pictures was very motivated to release the film, especially since they did not want to appear to be bullied. However the exogenous factor of a physical threat also played a role in the decision-making and is the additional modification to this hypothesis.

Despite law enforcement finding no credibility in the threat, major theatre chains were deterred by the threat of physical violence and the concern that they could be the next victim of cyberattacks should they agree to air the film. The preceding cyberattack lent a level of believability to the threat and the implied threat of future cyberattacks against the theatre chains that the private sector was not willing to chance and therefore they were deterred.

The extraordinary audience costs that Sony Pictures suffered in the wake of the cyberattack eventually resulted in the firing of Sony executive, Amy Pascal, as she detailed in interviews. Sony Pictures did retain her in another role, but the exposure of her communications made it impossible for the company to keep her in her leadership role. That is a significant consequence of the cyberattack and a noteworthy variable that ought to be included when assessing an aggressor's strategy in conducting cyber coercion.

In traditional coercive diplomacy, while an aggressor might choose to publicize a negotiation overture, that is distinctly different than airing someone's personal communications with their trusted confidants where they reveal the uglier sides of their private selves. Doing so, provides an advantage to the aggressor since the victim then has to manage both personal and professional crises, while wading through the spectrum of decision-making on how to respond to the aggressor's demand. In examining the key factors that influence the success or failure of cyber coercion, choices in the coercive strategy like ramping up audience costs for the victim, can be crucial in the context of the crisis. This hypothesis can be considered passing a hoop test.[452]

Hypothesis 3: If an aggressor chooses solely countervalue, soft or commercial targets that suffer higher audience costs and have few-to-zero counterattack options, and a fear of escalation, a victim is more likely to acquiesce to stop the pain and ward off future

[452] Van Evera, Stephen. Guide to the Methods for Student of Political Science. Ithaca: Cornell University Press: 31.

pain.

Status: Partial acceptance with modification

Explanation: For the case of Sony Pictures, this hypothesis also partially explains the outcomes and can be considered passing a hoop test.[453] It is a countervalue commercial target, it did suffer high audience costs, it did not have any counterattack options and, as the tranches of data were released over weeks, combined with the unsubstantiated threat of physical violence, Sony Pictures did have a fear of escalation. However, these factors alone, do not explain the outcome.

A combination of all three hypotheses best explains the outcome in the case of North Korea's cyber coercion against Sony Pictures. George's seven conditions that favor coercive diplomacy are a good starting point to explain this case but examining the four additional factors shows that they provided greater explanatory value in understanding the effectiveness of cyber coercion. Soft targets are easier to attack, face higher audience costs, and have to bear the financial burden themselves. Sophisticated attacks drive up the fear of escalation more than amateur attacks. Targeting the leadership can be both personally and professionally embarrassing and consequential for the leaders. Not only does the company leadership need to respond to the threat on behalf of the company, but they also have a self-interest in keeping their job when doing so, so they may be more willing to acquiesce to the pressure exerted by an aggressor. The addition of a subsequent physical threat along with the fear of the threat of potential additional

[453] Van Evera, Stephen. Guide to the Methods for Student of Political Science. Ithaca: Cornell University Press: 31.

cyberattacks against the theatre chains was noted by the theatre executives as the motivation to refuse to show the film. Without the extensive cyberattack preceding the unsubstantiated threat of violence, the threat of violence may not have been taken as seriously and may have failed because it would seem less credible. Each of these additional variables beyond George's original seven factors highlights important characteristics of an aggressor's cyber coercive strategy and how a victim may react.

Case of Russia vs. Estonia

Below is a table showing the changes of the independent variables across three temporal values for the Estonia-Russia case study. The dependent variable can be shown as an escalation spectrum of options over time. This dependent variable escalation spectrum is used to examine each dyad of cyber coercion over three temporal values. For the Russia-Estonia dyad below these are:

Time 1 – The initial period of Phase I of the attack – Estonia employed a combination strategy, first doing nothing and then defend.

Time 2 – Phase II of the attack - Estonia moved forward on its plan to relocate the statue and human remains and continued to defend itself while sustaining the more sophisticated Phase II of the cyberattack.

Time 3 – Six months post-attack - Estonia engaged in mounting a heavy defense, supplemented its modernized digital system to make it more difficult for Russia to hack in the future, received a NATO commitment to build a Cyber Centre of Excellence in Tallin and worked closer with the various CERT teams throughout Europe. For Estonia, its victimhood of cyber coercion resulted in creating a stronger defense while also not being compelled to acquiesce to the aggressor's demand.

Table 8:

RUSSIA – ESTONIA	
T0	The buildup to the conflict consisted of decades of historical and societal issues from Soviet invasion to the late 2006 proposal to relocate the monument and soldier remains from a central location to a distant cemetery
T1 Phase I	*Present IVs:* Targets: Countervalue including non-military government Nature: Amateurish in Phase I Leadership as a target; Attribution; Audience costs; Financial costs; Pressure on leadership; Clear objective; Strong coercer motivation; Sense of urgency; Adequate support; Clear and precise terms. *Not Present IVs:* No fear of unacceptable escalation
	Present DV: Coercer: Threat DV: status quo ante no action/no capitulation / no desired behavior change Result: Victim does not change behavior
T2 Phase II	*Present IVs:* Targets: Countervalue including non-military government Nature: Sophisticated in Phase II Leadership as a target; Attribution; Audience costs; Financial costs; Pressure on leadership; Clear objective; Strong coercer motivation; Sense of urgency; Adequate support; Clear and precise terms. *Not Present IVs:* No fear of unacceptable escalation
	Present DV: Coercer: Full cyberattack against multiple industries, financial institutions and government DV: status quo ante and defend by mitigating outages where possible by only allowing local traffic. no action/no capitulation / no desired behavior change Result: Victim does not change behavior nor acquiesce to demand; strengthens defenses.

Table 8 continued:

T3 Six months later	*Present IVs:* No on-going attack *Not Present IVs:* No fear of unacceptable escalation No asymmetry of motivation No targets
	Present DV: Coercer: The aftermath of the extended cyberattack against multiple industries, financial institutions six months prior. DV: Defend - strengthened defense; recognized need for increased cyber defenses in Estonia and throughout the region. Result: Victim still does not acquiesce to the demand and instead Estonia heavily invested in internal cyber defense, precluding future Russian cyber aggression and limiting future Russian cyber options. Further, this incident resulted in NATO creating a Cyber Centre of Excellence in Tallinn, concentrating cyber expertise at the center of the victim in this cyberattack. Estonia also partnered with its Nordic neighbors to extend best practices for cyber defense.

The conventional wisdom about the Russia-Estonia 2007 cyber conflict is that Estonia lost since Russia was able to successfully disrupt Estonian daily life for several weeks in late-April-May 2007. Re-examining this assumption reveals that claiming Estonia "lost" is a poor assessment of the situation when observed over a longer temporal value. Over time, Estonia's relative power and influence in the cyber realm increased, its ability to influence cyber policy in Europe increased, its own cyber defenses significantly increased, and it did not move the Bronze Soldier statue back to the city center. Further, Estonia was poised to assist Georgia when it was attacked the following year and was able to provide mirror websites, so Georgia was able to maintain a level of connectivity.

Hypothesis 1: George's seven conditions that favor coercive success (Clarity of the objective, Strength of Motivation, Asymmetry of Motivation, Sense of Urgency, Adequate Domestic and International Support, Opponent's Fear of Unacceptable Escalation, and Clarity Concerning Precise Terms of the Settlement of a Crisis) will fully explain the outcome.

Status: Reject

Explanation:

Similar to the North Korea vs. Sony Pictures case study, George's seven conditions are inadequate to account for all the factors affecting the outcome in the case of Russia vs. Estonia. The difference between a low-level attack like web defacement, seen in Phase I of the cyberattack against Estonia, compared with a high-level attack like paralyzing backbone servers, seen in Phase II, communicates two vastly different levels of threat to a victim. Similar to the Sony Pictures case study, targeting the soft targets in Estonia, in addition to the government targets was a strategic choice to ratchet up pressure, increase audience costs and increase financial costs, but unlike the Sony Pictures case, it did not work in Estonia.

The three additional factors that this case study unearthed as necessary to examine in a cyber coercive conflict are audience costs, financial costs and pressure on leadership. For Estonia, there were significant audience costs, but they were different in nature than what Sony suffered. For Estonia, it was not due to an embarrassing airing of private communications, it was embarrassing for the government that touted its digital expertise and digital reliability to have their systems overtaken by Russian actors. There were

audience costs for the response to Russia; quite simply, Tallinn could not acquiesce to Moscow's demands given the months-long Russian intimidation campaign against Estonia on this subject and of course Estonia's history and culture as a former republic of the Soviet Union. The Estonian leadership would look weak if it capitulated. Additionally, there were high audience costs because its society was unable to access basic services like media and banking that disrupted daily life. Given the extent of disruption to society for the Estonian citizens, the polity was much more cognizant of the on-going strife between Tallin and Moscow – and therefore there were higher potential audience costs – than would occur if a different strategy like economic sanctions or diplomatic threats had been Russia's strategy. At the same time, other instruments of coercion, like air strikes or a land invasion, would obviously impact the citizenry of this small Baltic nation more than an inability to access their banking systems and incur higher audience costs. The audience costs from cyber statecraft lean more toward the higher end of the scale when the targets of cyber coercion are entities that society relies upon for daily functioning and they are severely impacted.

The financial costs were also high, but a nation state government has a greater ability to absorb costs from an adversary attack (for those against the state infrastructure) than a company does who has to be responsive to a board. Since Estonia experienced both government and private industry targets, those soft targets like the media and banks did suffer financial costs. It is unknown if these costs by private industry were covered by insurance and therefore the costs were passed on to their insurers, if these private entities had to assume the costs themselves (and possibly make up for the loss by passing

part of the cost of the cyberattacks to their customers.)

There was obviously great pressure on the leadership but the Estonia leaders were not in jeopardy of losing their jobs due to this cyberattack in the way that the Sony executives were. One explanation for that is that the nature of cyberattacks differed greatly; in Estonia it was not personally humiliating like it was with Sony Pictures so while they both faced significant audience costs, Estonia escaped the additional layer of a public examination of personal, shameful internal communications.

While the Estonia leadership was a target, the nature of the attack against the Estonia leadership and parliament were lower-level attacks and therefore did not exert the same level of pressure on leadership as the public disclosures of sensitive internal documents did at Sony Pictures. The attribution factor was also satisfied in the Estonia case study, as described above.

Hypothesis 2: All other variables being equal, the greater the financial and/or audience costs faced by a victim where there is asymmetric motivation combined with a potential for leadership destabilization, the more likely the victim is to acquiesce to the demands of the aggressor over time.

Status: Reject

Explanation:

For this case study, the dyad did not display asymmetric motivation, but if we modify the hypothesis to account for equal motivation, it still does not explain the Estonian case. Estonia not only rejected the premise Russia's demand and refused to acquiesce, it defended itself and then went further to cooperate with regional partners to increase cyber defense for itself and throughout the region. With an equal motivation to the aggressor and a lack of targeting leadership with sophisticated attacks, the Estonian leadership had the space to figure out how to mitigate the attacks and then plan additional defense and formulate a strategy to increase regional cyber security.

If leadership had been undermined like it was at Sony Pictures, if trust in the government was damaged, if leadership was destabilized, we might have seen a different outcome in Estonia. However, the amateurish targeting of leadership in Estonia did not produce any concern over leadership destabilization so the leaders were not under personal attack nor personal pressure and were able to focus on how to lead the country through this attack.

Hypothesis 3: If an aggressor chooses solely countervalue, soft or commercial targets that suffer higher audience costs and have few-to-zero counterattack options, and a fear of escalation, a victim is more likely to acquiesce to stop the pain and ward off future pain.

Status: Reject

Explanation:

For this case study, the aggressor chose both soft, countervalue commercial and non-military government targets, but even with the modified addition of government countervalue targets, the rest of the hypothesis is not satisfied. Although Estonia's private sector was targeted heavily during this cyberattack, Estonia in 2007 had an advanced digital understanding and was able to defend and mitigate some of the consequences of the attack for both the government and private industry victims. Estonia may have experienced a fear of escalation if Russia supplemented the cyberattack with a threat of physical violence but given the months-long lobbying effort by the Russians against moving the statue, combined with the fraught history between the two nations in general and the high emotional content concerning this particular statue, Estonia was unlikely to capitulate based on the strategic and tactical choices Russia made in conducting this attack.

CHAPTER 7: CONCLUSION

There is no lasting peace in this game, no final battle determining the end. There is no victory banner hanging across a finish line to run through. In cyber statecraft, there are iterative games as the terrain, the technology, changes, and the opponents learn and adapt. There are only degrees of tension *ad infinitum* that states and non-state actors can use to their advantage, where possible.

This research counters the first wave pessimists and the second wave optimists and provides a Utilitarian theory of how factors involved in cyber statecraft can be effectively employed for coercive diplomacy. The comparative case studies of North Korea vs. Sony Pictures and Russia vs. Estonia victim decision-making shows a victim who partially acquiesces and one who not only refuses to be compelled but defends and then expands their defenses, partnering with neighboring countries and international alliances.

The first wave pessimists would consider cyber coercion to be alarming and be concerned about an overwhelming number of cyberattacks that could result in widespread damage. Conversely, the second wave optimists would deem cyber coercion as a fruitless nuisance, unable to be effective since the threat does not include bodily harm. The Utilitarian approach to cyber coercion shows that it can be effective, it can result in a victim changing its behavior, and can have consequences for international relations among adversaries. There does not need to be a fear that it will cause undue cyber chaos and result in extensive destruction, like the pessimists would reason. Nor should cyber coercion be dismissed as a pointless exercise that will never alter behavior, as the second

wave optimists would envision.

George's argument in *Forceful Persuasion* and *The Limits of Coercive Diplomacy* is that the individual circumstances in each coercive dyad determine the effectiveness of the attempt at coercive diplomacy and that there is no generalizable theory to extract to ensure a victim changes its behavior.[454] Instead, coercion is a fluid situation where critical factors being present or absent contribute toward its success or failure, but that each situation is unique. While George's seven conditions that favor coercive diplomacy begin to explain these divergent outcomes, this research extends his work with the addition of key variables for cyber coercion help to more fully explain the different outcomes observed in cyber coercion. The specific variables in the extended set include: 1) financial costs for the victim, 2) audience costs for the victim, 3) leadership destabilization potential through targeting of leadership, and 4) the amount of pressure on leadership. These additional factors extend George's approach to coercive diplomacy and adapts it for the advantages and drawbacks that cyber statecraft presents.

This research examined two case studies to illustrate how cyber coercion has been employed as a means of soft power in an attempt to achieve a specific outcome and how the extended set of variables help explain divergent outcomes. The first case is focused on North Korea's attempt at cyber statecraft to force Sony Pictures Entertainment to cancel the production and distribution of a satirical comedy film where the North Korean

---

[454] George, Alexander. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War.* Washington, DC: United States Institute of Peace Press, 1991; and, Alexander L. George and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994.

leader is a target of an assassination plot. This case is widely considered to be a failure for North Korea because the film was eventually released. However, this is also an incorrect characterization. Although the film was eventually released, after Sony Pictures decided to cancel it and then reversed that decision, it was a significantly pared down distribution that caused a financial loss in the tens of millions of dollars. Further, due to North Korea's actions, a Sony executive lost her job due to the ramifications of the attacks, Sony lost tens of millions of dollars on remediation and rebuilding their network, Sony lost an additional approximately $15 million due to lawsuits from former employees for the data breach, and it suffered an extreme public relations crisis due to its unsavory internal emails being published publicly. North Korea caused Sony Pictures to change its behavior from what it originally sought to do; Sony may not have complied with the full demand, but it did change its behavior due to the cyberattacks and associated threats.

From a Utilitarian standpoint, a recommendation for North Korea's strategy would not differ greatly from the strategy it pursued. The North Korean operation against Sony Pictures Entertainment shows that with the right strategy choices, it is possible for cyber statecraft to result in a victim changing its behavior over time. It may not result in a strict yes/no binary response to the coercer's demand, but instead it may result in partial compellence or deterrence. North Korea noiselessly stole the data in advance and then coerced Sony Pictures Entertainment not to air the film while also causing extensive destruction of Sony's systems, lending credibility to its talents and reinforcing the idea that it could continue to do harm. Pyongyang was able to disrupt the film's release by

imposing audience costs, financial costs, targeting leadership with a potential for destabilization, and by choosing a commercial countervalue target. North Korea slowly released the data in timed tranches thus building public interest over time and maximizing its publicity to pressure SPE, and strategically releasing categories of sensitive information in batches which continued to increase the pressure campaign, that also doxes and jeopardizes employees and associates. By slowly intensifying the pressure and supplementing this with an absurd threat of physical violence that, while found to be not credible and was unlikely to be taken serious without the extensive cyberattacks preceding it, still caused enough fear that the executives of the major cinema chains refused to air the film, North Korea's strategy was effective for its goals. While North Korea's ultimate goal of never airing the film was not achieved, it certainly achieved a level of effectiveness in relation to its demand. Its actions resulted in a pared down release of the film in question, a secondary deterrence of other studios making similar North Korean-focused films, cancelled promotional events, the firing of an American executive, a punitive public relations crisis and millions of dollars of destroyed computers. That is not a cancelling of the film, but that is significant damage inflicted on a company whose creation of a film the North Koreans perceived to be a direct threat.

For Sony's part, the Utilitarian view would be that it should have invested in cybersecurity protection for its vast computer network so that a sophisticated cyberattack like this could be hopefully detected at one of several levels. Beyond that, there have been extensive cybersecurity industry assessments written[455] that detail each step that

[455] For a complete accounting of the recommended critical controls that SPE lacked at the time,

Sony should have undertaken to reduce its risk along with critical controls it should have implemented long before the attack took place. Given the sheer amount of data that was stolen along with the extensive amount of physical damage done to its network, its cyber defenses were severely lacking.

The second case examined the use of cyber coercion by Russia to pressure Estonia not to move a statue, a move that Russia found particularly insulting to its military history. This incident is described as a success for Russia due to the widespread chaos the Russian actions caused throughout Estonia. However, this research has shown that this is an incorrect characterization. While Russia's actions were an attempt to dissuade Estonia from moving forward with its decision, the coercive measure backfired over time in some respects. This cyberattack caused Estonia not only to increase its defenses but caused NATO and Estonia's Nordic neighbors to unite with Estonia to create a robust partnership centered on cyber defense. Russia's dramatic attempt at cyber coercion resulted in the victim creating a stronger defense as well as banding with Russia's other adversaries and neighboring to defend themselves against any future cyber-based attacks. That being said, the attack on Estonia also allowed Russia to exercise its cyber capabilities in a way that it had not done prior in the breadth and depth of soft targets that it did in Estonia. From this, Russia was able to learn what worked and what did not, where it could improve, and to what extent it could disrupt cyberspace daily life before NATO responds. Russia used these lessons the following year when it

---

see Gabriel Sanchez. "Case Study: Critical Controls that Sony Should Have Implemented." *SANS White Paper*, June 1, 2015.

launched cyberattacks against Georgia and, later on, against Ukraine.

From a Utilitarian standpoint, Russia should not have engaged in such a public campaign if it truly wanted a chance to change minds about moving the statue. Given the complicated history between these nations, driving up the audience costs and the financial costs operates in opposition to Russia's stated goal; the more public and greater the disruption to the Estonian people, the less likely it was that the Estonian leadership would acquiesce. While ineffective for the stated goal, these cyberattacks allowed Russia to exercise its capabilities, allowed them to learn from their mistakes and best practices and adapt for future targeting, which has an important value. Further, it showed Russia what cyberspace damage they could inflict that did not result in a collective action from NATO. While not the goal of the coercion, these are beneficial consequences for Russia from its cyber coercive actions.

The defenses that Estonia implemented both in government and private sector were decently adept given the type of cyberattack launched initially. Since this was a first time instance, there was a learning curve, but they were able to restrict traffic to internal IPs and engage other mediation techniques that helped but did not solve the issue. More advanced cybersecurity, which is what Estonia invested in afterwards, would have been better to fend off aspects of this attack.

The extended variables with the greatest explanatory value for this case were audience costs, financial costs, and pressure on leadership. The audience costs for Estonia were high and functioned differently than in the case against Sony Pictures; Tallinn had no ability to acquiesce to Moscow, especially after the months of lobbying

and bullying from Moscow about the plan to move the statue, without suffering severe blowback from the Estonian constituents. Further, a significant attack on the nation's infrastructure, for the country that was considered the most digitally-forward in Europe at the time, incurred extensive audience costs based on the disruption of daily life for the typical Estonian. The high level of disruption that touched most Estonians backfired for Russia and served to bolster opinion against Russia's demands. Whereas, if Russia chose a different cyber statecraft strategy and selected targets that were less essential for daily life, they might have been more successful in their coercive efforts or, at least, these choices would not have engendered the extreme defensive posture Estonia adopted and may not have resulted in the NATO and Nordic partner's attention and investment in cyber defense.

The financial costs suffered were also high and since the targets were both government and commercial entities, these costs were split between the government and the private entities. There was high pressure on the Estonian leadership during this timeframe to restore access to the trusted digital infrastructure, to stand up to the Russians, to

The pressure on leadership was high but focused on navigating the two phases of the attack while still maintaining the confidence of the people in their trusted digital infrastructure. Unlike the Sony case study, the personal attack on leadership was amateurish in nature and did not cause much angst among the leadership. Due to the country's digital reliance and investment, the leadership was focused on restoring access, reestablishing trust in the digital infrastructure, and then strengthening its defenses and

resiliency. The cyberattack by Russia highlighted Estonia's cyber vulnerabilities and instead of acquiescing to Russia's demand, Estonia maintained its plan to move the statue. The 2007 cyberattack resulted in Estonia garnering support for increased collaboration on cybersecurity, the creation of the NATO CCDCOE in Tallinn, and getting Nordic partners focused on the threat of cybersecurity . Russia chose a cyber coercive strategy to maximally disrupt daily life and it backfired horribly for purposes of the coercive goal.

General Findings

This research provided four contributions: first, it provided an extended set of four variables that favor coercive diplomacy in the cyber realm and showed how these additional variables effect outcomes specific to cyber coercion. Second, this research provided a fused social science and cybersecurity method to understanding and obtaining attribution and surmount the purported obstacle that attribution poses to employing cyber coercion. Third, it provided evidence to support a Utilitarian theory of employing cyber coercion and showed that examining a cyber coercive act *over time* may provide additional data points and result in a different interpretation of the nature of a cyber coercive interaction. That is, a victim may modify their behavior later on, even if they do not immediately do so, and it is important to include the longer-term behavior changes when assessing the ramifications stemming from a coercive cyberattack. Last, this research showed that the conventional wisdom for two influential cases should be modified to account for the additional data gained by examining the case over a longer time period. These case studies have shown that it is the specific pressures involved in the coercive campaign that contribute to *how* and *to what degree* a victim may modify their behavior, that behavior may change over time, and it is not always to the benefit of the aggressor if this happens.

The additional variables that favor cyber coercive acts audience costs, financial costs, leadership as a target with potential leadership destabilization, and pressure on leadership. The nature of the attack also matters. Amateurish attacks are not taken as seriously as a sophisticated attack. Short attacks do not exert as much pressure as long,

drawn out attacks. The victim's concern over time is a significant factor; it is not just about their initial reaction it is how their motivation changes over time as the coercive cyber operation persists, the pressure builds, and financial and audience costs increase. Countervalue targets are often easier to attack and targeting leadership, with the goal of leadership destabilization, can contribute to a victim changing its behavior faster.

This research provided a strategy to surmount the attribution obstacle. Bringing together Healey's Spectrum of State Responsibility with Sharp's Known Coercer model and combining that with the forensic cybersecurity technical data and analysis denoting intrusion cluster attribution and/or country attribution combines a social science method with the best practices from the commercial cybersecurity industry to determine attribution. This hybrid method provides a holistic approach to the problem of attribution, fusing the approaches of social science with the technical insight from cybersecurity based on commercial cybersecurity industry techniques, forensics and databasing. This attribution strategy means that the "insurmountable challenge of attribution" that some researchers rely on to say that assessing cyber coercion is impossible, is now possible.

The third original contribution of this research is to look at victim responses over time instead of simply looking at a single point in time. This research illustrated problems with the conventional wisdom that is centered on winners and losers in a cyber coercive act and showed that examining what factors contribute to a spectrum of victim responses *over time* produced a different result than the simplified, one instance look in time would suggest. Looking across different temporal values illuminates circumstances that previous scholarship has ignored where the victim later changed their behavior. This is important

because it shows that the initial interpretation about how we understand the outcome of a coercive dyad can change drastically when viewed over a longer time period.

The in-depth nature of these case studies and the supporting evidence from cybersecurity forensics, primary and secondary documents and interviews with the leaders responsible for the decision-making lends confidence to the findings. This research advances a rethinking of how we analyze cyber coercive cases in terms of degrees of victim responses, and with the added perspective of looking at a case over time, the determination on what is effective and why may change drastically, instead of a simple binary interpretation.

With respect to the financial costs, while targeting countervalue government targets means that the government will likely absorb the costs associated with the cyberattack, when targeting private industry, those costs are often passed on to the insurance industry. Competent defense of a soft target's cyber systems is a costly endeavor, especially when it includes training all personnel in cyber hygiene practices (i.e. not click on the wrong phishing link), in addition to expensive technical defenses. A commercial entity may find it easier to purchase insurance and pass the cost on to a third party instead of investing in their own cyber defenses. Provided a company is insured, this is the outcome that is often seen in recent cybercrime cases of ransomware.

Implications for Future Policy Work

In terms of future research, especially looking at policies centered on cyber statecraft applied to commercial soft targets, this research has revealed several avenues that merit further scholarly investigation. One recommendation is a renewed focus on third wave cyber statecraft research; dispense with the concerns that cyber statecraft will cause massive destruction or that with no lethality it has no purpose and examine all the ways that states can use cyber statecraft to achieve its goals and for its benefit. What other factors that contribute to successful cyber coercion can be discovered by examining additional cases in-depth?

Targeting commercial, soft target entities for cyber statecraft purposes is a dangerous precedent from a policy perspective and requires a strong, punitive policy response. Both the Sony Pictures Entertainment and the Estonia case studies reveal a strategy that highlights the vulnerability of commercial entities and asserts that they are easier to target than a state. In addition, the lesson from the Sony Pictures cyberattack made the case for would-be coercers for a "hack and leak" strategy against commercial entities. While it might provide a means for a state to achieve its goals, targeting commercial entities and using hack and leak tactics is a destabilizing practice for offensive cyber operations, but also a critical perspective to understand for defensive cyber operations.

Future policy work should include disincentives for the hack and leak model and related behaviors. States ought to seek and work toward increased stability in cyberspace and that includes finding ways to disincentivize states from targeting commercial entities,

hacking and revealing their internal communications. Targeting commercial entities with cyberattacks does not increase cyberspace stability. However, the Sony Pictures case study showed that in this particular dyad, with the distinct strategic decisions that North Korea made in the conduct of this cyberattack, it resulted in the victim partially changing its behavior. This means that disincentivizing this behavior, especially when it provides a modicum of effectiveness, can be very difficult. Furthermore, future policy work ought to address disincentives for the individuals who publish the stolen data and doxing information. While this is extremely difficult in practice, from a policy perspective it ought to be addressed.

Taking the concept of policy disincentives a step further, it is one thing for a state to create policy to deter these activities inside its borders, but quite another for international agreements to codify these parameters and punishments and incorporate an enforcement mechanism. Future policy work ought to focus not only on creating policies to disincentivize this behavior but ensure wide adoption among states with a means to enforce and punish those who run afoul of it.

In looking at the case of Estonia, the attacks on its digital infrastructure and commercial, soft targets were so extensive that identifying the victims and the magnitude of the cyberattacks was widely reported. However, the commercial industry has learned and adapted; that is, they have learned that disclosing that they are the victim of a cyberattack can have financial consequences and have adapted by concealing this information from the public and, oftentimes, handing it quietly with their insurance company and/or cybersecurity incident response team. Another area for future policy

work would be on public reporting requirements for commercial targets to disclose when they have been the victim of cyber coercion or cyberattacks so that a more accurate understanding of the broad use of this strategy as well as the specific tactics involved can be thoroughly understood and examined.

Why is cyber statecraft and cyberattacks allowed to happen in the international system? There are divergent paths that states are taking with regard to the approach to cyber statecraft: European powers are largely leaning toward creating international institutions to agree to norms of behavior and may act as a policing function. While other powers in the international system do not want to be restricted and/or do not see a value in participating in such institutions since their adversaries are not limited in how they exercise their cyber power. Harkening back to the earlier discussion on Realism versus International Institutionalism illuminates the tension between these two schools of thought and can be applied to the notion of cyber statecraft. Further, the chapter on the origins of the internet shows how difficult it is to police this ever-changing technological terrain, and that difficulty has significant policy implications.

However, it is each state's self-interest to invest in the stability of cyberspace and build a cooperative cybersecurity coalition. Doing so supports freedom of speech, protects the free flow of commerce, and allows for information sharing, while still providing options to use cyber statecraft. While there are states that are reluctant to sign on to agreements like the Paris Call for Trust and Security in Cyberspace, one policy recommendation would be to consider negotiating tiers of international agreements, with the goal to eventually have everyone sign on to the full agreement. The case study on

Russia versus Estonia showed that Russia was able to act with impunity at the time. That is not to say that signing onto an international agreement that lacks an enforcement mechanism would restrain a state, like Russia, who believed the cyber statecraft activity was in its best interest, but

In order to increase participation in cybersecurity institutions, work with countries who refuse to join to find out what the individual disagreement points are and find a negotiated solution, perhaps a tiered version of the agreement. It will allow these reluctant nations to be part of the conversation with the goal of eventually signing onto the full agreement.

The cyber landscape is vast, constantly shifting and the policy world is rushing to catch up. As shown in the case studies, cyber coercion can impose high costs on a victim. Cyber resiliency, upgrading the internet infrastructure where possible, focusing on securing critical systems and improving cyber infrastructure defenses are policy areas that deserve additional attention. Similar to the attribution strategy laid out in this research, a policy recommendation is that a hybrid expertise approach would be most appropriate. That is, formulating policy to manage these issues should be devised by hybrid teams of policy experts and cybersecurity professionals in order to appropriately account for all aspects of this considerable challenge.

BIBLIOGRAPHY

"A Breakdown and Analysis of the December 2014 Sony Hack." *Risk Based Security*, December 5, 2014. Located at: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning and accessed on December 16, 2018.

"Advanced Persistent Threat Groups." *FireEye*. Located at: https://www.fireeye.com/current-threats/apt-groups.html and accessed on January 15, 2021.

"ARPANET." Defense Advanced Research Project Agency. Located at: https://www.darpa.mil/attachments/ARPANET_final.pdf . Accessed February 2, 2020

"Backdoor.Destover." *Symantec Security Center,* December 3, 2014.

"Bucharest Summit Declaration." *North Atlantic Treaty Organization*. April 3, 2008. Section 47. Located at: https://www.nato.int/cps/en/natolive/official_texts_8443.htm and accessed January 3, 2019.

"Consolidated Financial Results Forecast for the Third Quarter Ended December 31, 2014, and Revision of Consolidated Forecast for the Fiscal Year Ending March 31, 2015" *Sony News and Information.* Tokyo, Japan. Located at: https://time.com/wp-content/uploads/2015/02/150204_sony.pdf and accessed on December 17, 2018.

"Cyberwar: War in the fifth domain." *The Economist*, June 1, 2010.

"Estonia: Defense Minister Says Bronze Soldier Had To Go." *Radio Free Europe*, May 9, 2007. https://www.rferl.org/a/1076363.html

"European Parliament resolution of 24 May 2007 on Estonia." European Parliament, Document RC-B6-0205/2007, Texts Adopted, Strasbourg, France.

"Ex-Sony Chief Amy Pascal Acknowledges She Was Fired." *NBC News*, February 12, 2015. Located at: https://www.nbcnews.com/storyline/sony-hack/ex-sony-chief-amy-pascal-acknowledges-she-was-fired-n305281

International Telecommunications Union, Statistics. Located at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Accessed on February 2, 2021.

"Lazarus Under the Hood." *Kaspersky Labs*, 2018. Located at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

"NATO Opens New Center of Excellence on Cyber Defense." *NATO News*, May 14, 2008. Located at: https://www.nato.int/docu/update/2008/05-may/e0514a.html and accessed on January 3, 2019.

"North Korea." Freedom House, 2017. Located at: https://freedomhouse.org/country/north-korea/freedom-world/2017 and accessed on December 18, 2019

"North Korea Stages Show of Force with New Missiles During Parade," *Reuters,* September 9, 2018. https://www.reuters.com/article/us-northkorea-missiles-parade/north-korea-stages-show-of-force-with-new-missiles-during-parade-idUSKBN1FT0U8 Accessed September 20, 2019.

"Protecting the Cybersecurity of America's Networks." *The Brookings Institution*. February 11, 2021. Located at: https://www.brookings.edu/blog/techtank/2021/02/11/protecting-the-cybersecurity-of-americas-networks/

"Russia Cuts Oil Product Exports via Estonia-source." Reuters, May 4, 2007.

"Sony Cancels 'Interview' Release After Theatres Drop Out While Fox Folds Similar Movie." NBC News, December 17, 2014. Accessed via https://www.nbcnews.com/storyline/sony-hack/sony-cancels-interview-release-after-theaters-drop-out-while-fox-n270281 on April 2, 2018.

"Tallinn tense after deadly riots." BBC News, April 28, 2007. http://news.bbc.co.uk/2/hi/europe/6602171.stm

"The cyber raiders hitting Estonia." BBC News, May 17, 2007. Located at: http://news.bbc.co.uk/2/hi/europe/6665195.stm and accessed on November 23, 2019.

"The History of the Internet" via The Department of Computer Science Old Dominion University. Located at: https://www.cs.odu.edu/~tkennedy/cs300/development/Public/M02-HistoryOftheInternet/index.html#:~:text=1965%3A%20Working%20with%20Thomas%20Merrill,area%20computer%20network%20ever%20built and accessed February 1, 2021.

"Russia." Freedom House, 2007. Located at: https://freedomhouse.org/report/freedom-world/2007/russia and accessed on December 18, 2019.

Achen, H. and Duncan Snidal. "Rational Deterrence Theory and Comparative Case Studies." *World Politics* Vol. 41, No. 2 (Jan., 1989): 143-169.

Alexander, Bryan, Andrea Mandell & Elizabeth Weise. “No 'Interview' ... on any platform.” *USA Today*, December 17, 2014.

Alperovitch, Dmitri. “Revealed: Operation Shady RAT.” *McAfee White Paper*, 2011. http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf

Alperovitch, Dmitri. “Unprecedented Announcement by FBI Implicates North Korea in Destructive Attacks” Crowdstrike, December 16, 2014. Located at: https://www.crowdstrike.com/blog/unprecedented-announcement-fbi-implicates-north-korea-destructive-attacks/ and accessed December 20, 2018

Anderson, Nate. “Massive DDoS attacks target Estonia; Russia accused.” *ArsTechnica*, May 14, 2007. Located at: https://arstechnica.com/information-technology/2007/05/massive-ddos-attacks-target-estonia-russia-accused/ and accessed on November 2, 2019.

Arntz, Pieter. “Explained: Advanced Persistent Threat” *MalwareBytes Labs*, July 26, 2016. Located at: https://blog.malwarebytes.com/101/2016/07/explained-advanced-persistent-threat-apt/ and accessed on January 15, 2021.

Arquilla, John and David Ronfeldt. “Information, power and grand strategy: in Athena’s camp.” *In Athena’s Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, 1997.

Arquilla, John and David Ronfeldt, “Cyberwar is Coming!” *Comparative Strategy*, Vol 12, No. 2 (Spring 1993).

Arreguin-Toft, Ivan. "How the Weak Win Wars: A Theory of Asymmetric Conflict." *International Security*, Vol. 26, No. 1 (Summer 2001).

Art, Robert J. “To What Ends Military Power.” *International Security* 4, No. 4 (Spring 1980).

Axelrod, Robert and Rumen Iliev. “The Timing of Cyber Conflict.” *Proceedings of the National Academy of Sciences of the United States of America.* Vol. 111, No. 4 (January 28, 2014): 1298-1303. https://doi.org/10.1073/pnas.1322638111

Beaumont-Thomas, Ben. “North Korea complains to UN about Seth Rogen comedy The Interview.” *The Guardian*, July 10, 2014. Located at: https://www.theguardian.com/film/2014/jul/10/north-korea-un-the-interview-seth-rogen-james-franco

Bennett, Andrew. "Process Tracing and Causal Inference." *Rethinking Social Inquiry: Diverse Tools, Shared Standards*, edited by Henry Brady and David Collier. Plymouth, UK: Rowman & Littlefield Publishers; Second edition, 2010.

Bennett, Andrew, and Jeffrey T. Checkel. “Process Tracing: From Philosophical Roots to Best Practices.” *In Process Tracing: From Metaphor to Analytic Tool*, edited by Andrew Bennett and Jeffrey T. Checkel, 3–38. From the Series: Strategies for Social Inquiry. Cambridge: Cambridge University Press, 2014.

Bennett, Bruce. “Did North Korea Hack Sony?” *RAND,* December 11, 2014.

Berninger, Matt. “Going ATOMIC: Clustering and Associating Attacker Activity at Scale.” *FireEye,* March 12, 2019. Located at: https://www.fireeye.com/blog/threat-research/2019/03/clustering-and-associating-attacker-activity-at-scale.html and accessed on January 15, 2021.

Betz, David J. and Tim Stevens, “Analogical Reasoning and Cyber Security,” *Security Dialogue,* Vol. 44, No. 2, (April 2013): 147–164.

Bradley, Tony. “CrowdStrike demonstrates how attackers wiped the data from the machines at Sony.” *CSOnline*, February 4, 2015. Located at: https://www.csoonline.com/article/2880095/crowdstrike-demonstrates-how-attackers-wiped-the-data-from-the-machines-at-sony.html and accessed on December 3, 2018.

Bright, Arthur. “Estonia Accuses Russia of ‘cyberattack’.” *CSMonitor*, May 17, 2007.

Bratton, P. “When is coercion successful? And why can't we agree on it?” *Naval War College Review*, Vol. 58, No. 3 (2005): Article 6. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2050&context=nwc-review

Brinded, Lianna. “The Interview Tipped to Cost Sony Pictures $200 Million Following Hack and Cancellation.” *International Business Times*, December 18, 2014

Bumiller, Elizabeth and Thomas Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times,* October 11, 2012.

Byman, D and M Waxman. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might.* UK: Cambridge University Press, RAND, 2002.

Calamur, Krishnadev. “Theater Cancels New York Premiere of 'The Interview'.” *NPR,* December 16, 2014. https://www.npr.org/sections/thetwo-way/2014/12/16/371259776/amid-threats-by-hackers-actors-pause-promotion-of-sony-movie

Cieply, Michael and Brooks Barnes. “Sony’s Dirty Laundry, For All to See.” *The New York Times*, December 11, 2014.

Cisco Annual Internet Report (2018-2023) White Paper. March 9, 2020. Located at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed January 8. 2021.

Cisco Products. "What are the Most Common Cyber Attacks?" Located at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html and accessed on November 6, 2019

Clarke, Richard and Robert Knake. *Cyber War: The Next Threat to National Security and What To Do About It*. New York: Harper Collins, 2010.

Clayton, Richard, Steven J. Murdoch, and Robert N.M. Watson, "Ignoring the Great Firewall of China," paper presented at the Sixth Workshop on Privacy Enhancing Technologies, Robinson College, Cambridge, United Kingdom, June 28–30, 2006.

Cohen-Almagor, Raphael. "Internet History." *International Journal of Technoethics,* Vol. 2, No. 2, (April-June 2011): 45-64.

Collier, David. "Understanding Process Tracing." *PS: Political Science and Politics,* Vol. 44, No. 4 (October 2011).

Collier, David (ed.) "Case Selection, Case Studies, and Causal Inference: A Symposium." *Newsletter of the APSA Organized Section for Qualitative and Mixed-Method Research,* Vol. 2 (2008):2-16

Collier, David and James Mahoney. "Insights and Pitfalls: Selection Bias in Qualitative Research." *World Politics,* Vol. 49, No. 1, (October 1996).

Cook, James. "Sony Hackers Have Over 100 Terabytes of Documents. Only Released 200 Gigabytes So Far." *The Business Insider,* December 16, 2014.

Craig, Gordon A. and Alexander George. *Force and Statecraft.* Oxford: Oxford University Press, 1995.

Crowdstrike Intelligence Report. "2015 Global Threat Report." *Crowdstrike,* 2015.

Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security." *International Journal of Cyber Warfare and Terrorism,* Vol. 1, No. 1, (January-March 2011): 24-34.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired,* August 21, 2007. Accessed via https://www.wired.com/2007/08/ff-estonia/ on October 26, 2018.

Day, Mark. December 17, 2014. Located at: https://twitter.com/MarkDayNews/status/545340141817315328.

Denning, Dorothy. *Information Warfare and Security* (Reading, MA: Addison-Wesley Longman, 1999).

De Moraes, Lisa and Nellie Andreeva. "'The Interview' Release: 331 Theaters Aboard For Christmas Day." *Deadline*, December 24, 2014. Located at: https://deadline.com/2014/12/interview-christmas-release-theaters-deadline-looms-1201334671/ and accessed on December 14, 2020.

Drezner, Daniel. "The Hidden Hand of Economic Coercion." *International Organization*, Vol. 57, No. 3, (Summer 2003): 643–659.

Elkind, Peter. "Inside the Hack of the Century." *Fortune Magazine* (New York, NY), June 25, 2015.

Evans, Ryan. "Is Cyber Half the Battle?" *War on the Rocks interview with Ben Buchanan, Erica Borghard and Fiona Cunningham*, podcast audio, May 12, 2020. https://warontherocks.com/2020/05/is-cyber-half-the-battle

Evron, Gadi. "Battling Botnets and Online Mobs Estonia's Defense Efforts During the Internet War." *Georgetown Journal of International Affairs*, Vol. 9, No. 1 (Winter/Spring 2008): 121–126.

Evron, Gadi. "Estonia 10 Years Later: Lessons learned from the World's First Internet War." Securityledger.com. April 28, 2017. Located at: https://securityledger.com/2017/04/estonia-10-years-later-lessonslearned-from-the-worlds-first-internet-war/

Farwell, James P. and Rafal Rohozinski. "The New Reality of Cyber War." *Survival*, Vol 54, No. 4.

Feeney, Nolan. "Sony Asks Media to Stop Covering Hacked Emails." *Time*, December 15, 2014.

Fearon, James. "Domestic Political Audiences and the Escalation of International Disputes." *American Political Science Review*, Vol. 88, No. 3, (September 1994): 577-592.

Flemming, Daniel and Neil Rowe. "Cyber Coercion: Cyber Operations Short of Cyberwar." *ICCWS 2015 - The Proceedings of the 10th International Conference on Cyberwarfare and Security*, p. 95–101. Edited by Jannie Zaaiman and Louise Leenan. 2015.

Fogleman, Ronald. Remarks as delivered by Gen. Ronald R. Fogleman, Air Force Chief of Staff, to the Armed Forces Communications-Electronics Association, Washington,

April 25, 1995. Located at: http://www.iwar.org.uk/iwar/resources/5th-dimension/iw.htm and accessed on June 1, 2018.

Ford, Dana and Madison Park. "North Korea to U.S.: Show evidence we hacked Sony." *CNN*, January 14, 2015

Fritz, Ben and Danny Yadron. "Sony Hack Exposed Personal Data of Hollywood Stars; Breach Includes Social Security Numbers for 47,000 Employees and Actors, Including Sylvester Stallone, Judd Apatow and Rebel Wilson. *The Wall Street Journal*, December 5, 2014.

Fritz, Ben, Erich Schwartzel and Barret Devlin. "Sony Pulls Korea Film "The Interview;" U.S. Blames Pyongyang for Hack; Studio Scraps Dec. 25 Debut After Terrorist Threats Prompted Movie Chains to Skip Film." *The Wall Street Journal*, December 18, 2014.

F-Secure White Paper. "The Dukes 7 Years of Russian Cyber Espionage," September 2015. https://blog.f-secure.com/the-dukes-7-years-of-russian-cyber-espionage/

Gallagher, Sean. "Who's Winning the Cyberwar – the squirrels, of course." *Ars Technica*, January 16, 2017. Found at: https://arstechnica.com/information-technology/2017/01/whos-winning-the-cyber-war-the-squirrels-of-course and accessed on November 27, 2020.

Gartzke, E. The Myth of Cyberwar. *International Security*, Vol. 38, No. 2, (Fall 2013): 41–73.

Gartzke, Eric and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace." *Security Studies*, Vol. 24 (2015):316–348.

Geddes, B. "How the Cases You Choose Affect the Answers You Get: Selection Bias in Comparative Politics." *Political Analysis* Vol. 2, No. 1, 1990.

Gerring, John. *Case Study Research: Principles and Practices (Strategies for Social Inquiry) 2nd Edition*. Cambridge: Cambridge University Press, 2017

Gerring, John. "What is a Case Study and What is it Good For?" *American Political Science Review*, Vol. 98, No. 2 (2004): 341-354.

Gerring, John and Lee Cojocaru. "Selecting Cases for Intensive Analysis: A Diversity of Goals and Methods." *Sociological Methods & Research*, Vol. 45, No. 3 (2016) 392-423.

George, Alexander. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. Washington, DC: United States Institute of Peace Press, 1991.

George, Alexander L. and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MIT Press, 2005.

George, Alexander L. and William E. Simons, eds., *The Limits of Coercive Diplomacy*, 2nd ed. Boulder, CO: Westview Press, 1994.

Gilmore, Jim. "Interview with Toomas Henrik Ilves." *Frontline*, June 23, 2017.

Gilpin, Robert. *War and Change in World Politics*, Cambridge University Press, 1981.

Glaser, Charles. "Realists as Optimists: Cooperation as Self-Help." *International Security*, Vol. 19, No. 3 (1994/95).

Glaser, Charles L. & Chaim Kaufmann: "What Is the Offense-Defense Balance and How Can We Measure It?", *International Security*, Vol. 22, No. 4 (Spring 1998): 44-82.

Goertz, Gary and James Mahoney's *Tale of Two Cultures: Qualitative and Quantitative Research in the Social Sciences*. Princeton, Princeton University Press, 2012.

Griffiths, James. *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. London: Zed Books, 2019.

Hall, Peter. "Tracing the Progress of Process-Tracing." *European Political Science*, Vol. 12, No. 1 (2013): 20-30

Harknett, Richard. Professor and head of the Department of Political Science, University of Cincinnati; presenting at the Cato Institute "Cyber Warfare, Coercion, and Restraint," May 9, 2019. https://www.cato.org/multimedia/events/cyber-warfare-coercion-restraint

Hare, Forrest. "The Cyber Threat to National Security: Why Can't We Agree?" *Conference on Cyber Conflict Proceedings, 2010.* Tallinn, CCD COE Publications.

Hare, Forrest. "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." *Fourth International Conference on Cyber Conflict,* 2012. Tallinn, CCD COE Publications.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Washington, DC: Cyber Conflict Studies Association, 2013.

Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." *The Atlantic Council*, January 2012.

Healey, Jason. "Winning and Losing in Cyberspace." In 2016 8th International Conference on Cyber Conflict Cyber Power, N. Pissanidis, H. Rõigas, M. Veenendaal, eds. Tallinn: NATO CCD COE Publications, 2016.

Hess, Amanda. "Inside the Sony Hack." *Slate,* November 22, 2015. Accessed via http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html on March 28, 2018. See also "Company-Wide Consequences of Sony's Data Breach" *Promisec Report, 2017.*

Hesseldahl, Arik. "Here's Sony Lawyer's Letter Telling Publishers to Stop Publishing Leaks." *Vox,* December 14, 2014. Located at: https://www.vox.com/2014/12/14/11633802/sony-demands-end-to-publishing-leaks-from-stolen-data

Hesseldahl, Arik. "Sony Pictures Investigates North Korea Link In Hack Attack." *Vox,* November 28, 2014. Located at: https://www.vox.com/2014/11/28/11633356/sony-pictures-investigates-north-korea-link-in-hack-attack

Hodgson, Quentin, Logan Ma, Krystyna Marcinek and Karen Schwindt. "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace." Santa Monica, CA: RAND. 2019. Located at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2961/RAND_RR2961.pdf

Ifill, Gwen. "Interview with Dmitri Alperovich and Mark Rogers." *PBS Newshour,* December 23, 2014. Located at: https://www.pbs.org/newshour/show/debating-north-koreas-involvement-sony-hack and accessed November 22, 2018.

Ignatius, Adi. "They Burned the House Down: An Interview with Michael Lynton Recovering from the most devastating hack in corporate history." *Harvard Business Review*, July–August 2015.

Ilves, Toomas Hendrik. 'Address by the President of Estonia' (62nd Session of the United Nations General Assembly, New York, September 25, 2007. https://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf

Ilves, Toomas Hendrik. 'Address by the President of Estonia' (67th Session of the United Nations General Assembly, New York, September 26, 2012. https://vp2006-2016.president.ee/en/official-duties/speeches/7991-address-by-h-e-toomas-hendrik-ilves-president-of-estonia-to-the-67th-session-of-the-united-nations-general-assembly-un-headquarters-new-york-september-2012/ and accessed June 2, 2019.

Ilves, Toomas Hendrik. Interview with Toomas Hendrik Ilves, President of Estonia, 2007 – 2016. "10 Years of Cyber Estonia: What will the Next Decade Bring?" *Center for Strategic and International Studies*, November 6, 2017.

Ilves, Toomas. "Prepared Testimony and Statement for the Record of Toomas Hendrik Ilves, President of Estonia 2006-2016 At the Hearing on 'The Modus Operandi and Toolbox of Russia and Other Autocracies for Undermining Democracies Throughout

the World.' Before the Senate Judiciary Subcommittee on Crime and Terrorism March 15, 2017. Located at: https://www.judiciary.senate.gov/imo/media/doc/03-15-17%20Ilves%20Testimony.pdf and accessed on June 10, 2019.

Israeli Defense Forces tweet: https://twitter.com/IDF/status/1125066395010699264.

Jervis, Robert. "Cooperation under the Security Dilemma." *World Politics*, Vol. 30, No. 2 (1978).

Jervis, Robert. "Realism, Neorealism and Cooperation: Understanding the Debate." *International Security*, Vol. 24, No. 1 (1999).

Johnson, A.L. "Endpoint Protection." *Broadcom*, May 26, 2016. Located at: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8ae1ff71-e440-4b79-9943-199d0adb43fc&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments and accessed on December 6, 2019.

Junio, Timothy. "How Probably is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate." *The Journal of Strategic Studies*, Vol. 36, No. 1, (2013): 130.

Kaljulaid, Kersti, President of Estonia, remarks presented at "Deciding on the Rules of the Road for Cyberspace: The Who, What, Where, When, How" at the Institute of International Cyber Stability, June 9. 2020. https://www.youtube.com/watch?v=DANP9AehqXs

Kang, Cecelia. "Sony Pictures co-chair Amy Pascal steps down." *Washington Post*, February 5, 2015.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War.* New York: Simon and Schuster, 2017.

Kattel, Rainer and Ines Mergel. "Estonia's Digital Transformation," in *Great Policy Successes.* Compton, Mallory E.; Hart, Paul. Oxford : Oxford University Press, 2019.

Kello, Lucas. "The Meaning of the Cyber Revolution." *International Security*. Vol. 38, No. 2, (Fall 2013).

Keohane, Robert. *After Hegemony*. Princeton, NJ: Princeton University Press. 1984

Keohane, Robert. "The Demand for International Regimes." *International Organization*, Issue 36, No. 2. (Spring 1982).

Keohane, Robert and Lisa Martin. "The Promise of Institutionalist Theory." *International* Security, Vol. 20, No. 1 (Summer, 1995): 39-51

King, Gary, Robert Keohane and Sidney Verba. *Designing Social Inquiry: Scientific Inference in Qualitative Research.* Princeton: Princeton University Press, 1994.

Kleinrock, Leonard. “Information Flow in Large Communication Nets: Proposal for a PhD Thesis.” Massachusetts Institute of Technology, May 31, 1961.

Koh, Harold Hongju. “The Emerging Law of the 21st Century War.” *The Brookings Institute*. Breyer Lecture presentation, April 1, 2016.

Krebs, Brian. “In Damage Control, Sony Targets Reporters.” *Krebs on Security*, December 15, 2014. Located at: https://krebsonsecurity.com/2014/12/in-damage-control-sony-targets-reporters/ and accessed December 21, 2018.

Kurose, J. F. and K. W. Ross. *Computer Networking: A Top-Down Approach*, 5th Edition. New York: Addison Wesley, 2010.

Lang, Brent. "‘The Interview’ Makes $40 Million Online and On-Demand." *Variety*, January 20, 2015.

Lang, Brett. “Sony Hack ‘Unparalleled and Well-Planned Crime,’ Cyber Security Firm Says.” *Variety*, December 6, 2014.

Lee, Edmund. “You Will Get to See "The Interview," Sony Lawyer Says.” *Vox*, December 21, 2014.

Lewis, James A. “A Note on the Laws of War in Cyberspace.” *Center for Strategic and International Studies*, April 2010.

Lewis, James. “Toward a More Coercive Cyber Strategy.” *Center for Strategic and International Studies*, March 4, 2021.

Levy, Jack. “Deterrence and Coercive Diplomacy: The Contributions of Alexander George.” *Political Psychology*, Vol. 29, No. 4, (2008): 537-552.

Libnicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009; National Research Council, ed., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010).

Libicki, Martin. *What is Information Warfare*. Government Printing Office, 1995.

Licklider, JCR and Welden Clark. “On-line Man-Computer Communication. *Proceedings of the Spring Joint Computer Conference.* Archived at the Internet

Archive and located at: https://archive.org/details/online-man-computer-communication/page/n3/mode/2up

Lieber, Keir. “The Offense-Defense Balance and Cyber Warfare,” in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies.* Monterey, CA: Naval Postgraduate School, 2015: 96–107.

Lieff, Cabraser, Heimann and Bernstein. “Sony Data Breach.” Located at: https://www.lieffcabraser.com/privacy/sony-data-breach/. See also Dominic Patten. “Sony Hack Class Action Settlement Gets Final Approval.” *Deadline,* April 6, 2016.

Liff, Adam. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.” *Journal of Strategic Studies,* Vol. 35, No. 3, (2012): 401-428.

Lin, Herb. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* Vol. 94, No. 886, (Summer 2012): 515-531.

Lin, Herbert. “Oft-Neglect Cost Drivers of Cyber Weapons,” Council on Foreign Relations Net Politics (online blog), December 14, 2016, http://blogs.cfr.org/cyber/2016/12/14/oftneglected-cost-drivers-of-cyber-weapons/

Lin, Patrick, Fritz Allhoff, and Neil Rowe. "Is It Possible to Wage a Just Cyberwar?" *The Atlantic Monthly,* June 5, 2012. Found at http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106 and accessed September 4, 2013.

Lindsay, Jon R. "The Impact of China on Cybersecurity." *International Security,* Vol. 39, No 3.

Lindsay, Jon. “Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack.” *Journal of Cybersecurity*, Vol. 1, No. 1, (2015): 53–67

Lindsay, Jon and Erik Gartzke. “Coercion through Cyberspace: The Stability-Instability Paradox Revisited.” In Kelly M. Greenhill and Peter J. P. Krause, eds., *The Power to Hurt: Coercion in Theory and in Practice.* New York: Oxford University Press, 2018.

Lynn-Jones, Sean. “Does Offense-Defense Theory Have a Future?” Based on a talk delivered to the Research Group in International Security at McGill University on October 20, 2000. https://www.researchgate.net/publication/265287636_Does_Offense-Defense_Theory_Have_a_Future

Mahoney, James. “After KKV: The New Methodology of Qualitative Research” *World Politics* Vol. 62, No. 1 (January 2010): 120-147.

Mahoney, James and Gary Goertz. The Possibility Principle: Choosing Negative in Comparative Research. *American Political Science Review* Vol. 98, No. 4 (November 2004): 653-669.

Mardiste, David. "Russia to Estonia: Don't Move Our Statue." *Reuters*, January 25, 2007. https://www.reuters.com/article/us-estonia-russia-statue/russia-to-estonia-dont-move-our-statue-idUSL2378719620070125 and accessed on November 11, 2019.

Mathews, Lee. "Florida Water Plant Hackers Exploited Old Software And Poor Password Habits." *Forbes*, February 15, 2021. Located at: https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poor-password-habits/?sh=3514b8b5334e and accessed on February 21, 2021

McNary, Dave. "Amy Pascal Talks Getting 'Fired,' Sony Hack and Angelina Jolie Emails in Candid Interview." *Variety*, February 11, 2015.

McNary, Dave. "Sony Has 'No Further Release Plans' for 'The Interview'." *Variety*, December 17, 2014.

Mearsheimer, John. "The False Promise of International Institutions." *International Security*, Issue 19, No. 3. (Winter 1994/1995): 5-49.

Mearsheimer, John. *The Tragedy of Great Power Politics*, New York: Norton, 2001.

Menn, Joseph. "Symantec Says 'Highly Likely' North Korea group behind ransomware attacks." *Reuters*, May 22, 2017. Located at: https://www.reuters.com/article/us-cyberattack-northkorea/symantec-says-highly-likely-north-korea-group-behind-ransomware-attacks-idUSKBN18I2SH and accessed on December 6, 2019.

Miller, Daniel. "Future of Sony's Amy Pascal questioned after hacked email revelations." *Los Angeles Times*, December 11, 2014.

Mite, Valentinas. "Estonia: Attacks Seen as First Case of 'Cyberwar'." *Radio Free Europe/Radio Liberty*, May 30, 2007. https://www.rferl.org/a/1076805.html

Mochizuki, Takashi. "Sony Head Thanks Supporters in Hacking Attack." *Wall Street Journal*, January 5, 2015.

Nakamitsu, Izumi, Under-Secretary-General and High Representative for Disarmament Affairs, United Nations, remarks presented at "Deciding on the Rules of the Road for Cyberspace: The Who, What, Where, When, How" at the Institute of International Cyber Stability, June 9. 2020. https://www.youtube.com/watch?v=DANP9AehqXs

NATO Strategic Communications Centre of Excellence. “2007 cyberattacks on Estonia” Located at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf and accessed on November 24, 2019.

Nazario, Jose. “Estonian DDoS Attacks – A summary to Date.” Published on Netscout Arbor, May 17, 2007.

Neuman, Scott. “North Korea Threatens War Over New Seth Rogen Comedy.” *NPR*, June 25, 2014. https://www.npr.org/sections/thetwo-way/2014/06/25/325646474/north-korea-threatens-war-over-new-seth-rogen-comedy See also “DPRK accuses U.S. film of insulting its leadership” *Xinhua*, June 25, 2014.

Nichols, Michelle. “North Korea says "wait and see" when asked about Sony hacking.” *Reuters*, December 1, 2014. https://www.reuters.com/article/us-sony-cybersecurity-northkorea/north-korea-says-wait-and-see-when-asked-about-sony-hacking-idUSKCN0JF2UJ20141201

Norton Products. https://us.norton.com/online-threats/glossary/p/password-based-attack.html. Accessed on December 16, 2019.

Nye, Joseph. "Deterrence and Dissuasion in Cyberspace." *International Security,* Vol. 41, No. 3. (Winter 2016/2017).

Nye Jr., Joseph. “”Nuclear Lessons for Cybersecurity?” *Strategic Studies Quarterly*, Winter 2011.

Nye, Joseph. "Information Warfare versus Soft Power." *Project Syndicate*, Prague, May 2017.

Osborne, Charlie. “Sony hires FireEye's Mandiant following internal security breach.” *ZDNET*, December 1, 2014.

Ottis, Rain. “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.” *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia. 2008.

Owens, William, Kenneth W. Dam and Herbert S. Lin (eds.), ‘Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.’ Washington, DC: The National Academies Press, 2009.

Oxford English Dictionary. OED Online. June 2019. Oxford University Press. http://www.oed.com/viewdictionary

Paet, Urmas. “Declaration of the Minister of Foreign Affairs of the Republic of Estonia.” May 1, 2007. Located at: https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia and accessed on November 22, 2019.

Pape, Robert. *Bombing to Win: Air Power and Coercion in War*. Cornell University Press, 1996.

Pape, Robert. “The True Worth of Air Power.” *Foreign Affairs,* Issue 2 (March/April 2004): 116-130

Peralta, Eyder. “Obama Says Sony Should Not Have Pulled Film Over Threats.” *National Public Radio,* December 19, 2014

Peterson, Andrea. “Sony Pictures Hackers Invoke 9/11 While Threatening Theaters that Show ‘The Interview’.” *The Washington Post,* December 16, 2014.

Pew Research, https://www.pewresearch.org/fact-tank/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/

Putin, Vladimir. ”Speech at the Military Parade Celebrating the 62nd Anniversary of Victory in the Great Patriotic War,” Kremlin transcripts, May 9, 2007. Located at: http://en.kremlin.ru/events/president/transcripts/24238 and accessed on November 21, 2019.

Quester, George. “Offense and Defense in the International System.” In Michael Brown, Owen Cote Jr., Sean Lynn-Jones, and Steven Miller (eds.) *Offense, Defense and War*. Cambridge: MIT press, 2004.

Quester, G. H. (1977). *Offense and Defense in the International System*. New York: John Wiley & Sons.

Ragan, Steve. “Sony's IT blueprints leaked by hackers.” *CSO Online,* December 4, 2014. Located at: https://www.csoonline.com/article/2855005/sonys-it-blueprints-leaked-by-hackers.html

Republic of Estonia, Ministry of Foreign Affairs. “Estonian Ambassador to Moscow was attacked.” May 2, 2007. Located at: https://vm.ee/en/news/estonian-ambassador-moscow-was-attacked and accessed on November 19, 2019.

Ricks, Jacob and Amy Liu. “Process-Tracing Research Designs: A Practical Guide.” *PS: Political Science & Politics,* Vol. 51, No. 4 (October, 2018): 842–846. https://doi.org/10.1017/S1049096518000975

Rid, T. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* Vol. 35, No 1 (2012): 5-32.

Rid, Thomas. “Cyberwar May Not Happen.” Located on the author’s website at: https://ridt.co/wp-content/uploads/2011/10/Rid-KCL-comment.pdf and accessed on June 3, 2021.

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks.” *The Journal of Strategic Studies.* Vol 38, No 1-2.

Rogen, Seth. June 25, 2014. https://twitter.com/Sethrogen/status/481811214737997825

Rothman, Michael and Jason Nathanson, "Sony Pulls the Plug on Dec. 25 Release of 'The Interview' After Threats." *ABC News*, December 17, 2014. https://abcnews.go.com/Entertainment/sony-pulls-plug-dec-25-release-interview/story?id=27675761

Ruus, Kertu. “Cyberwar I: Estonia Attacked from Russia.” *European Affairs*, Vol. 9, Issue 1, (Winter/Spring 2008).

Sagan, Scott. “Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb” *International Security*, Vol. 21, No. 3.

Gabriel Sanchez. “Case Study: Critical Controls that Sony Should Have Implemented.” *SANS White Paper*, June 1, 2015.

Schelling, Thomas. *Arms and Influence.* New Haven: Yale University Press, 1966.

Schelling, Thomas. "The Diplomacy of Violence." *Essential Readings in World Politics*, Karen Mingst and Jack Snyder, eds. New York: WW Norton & Company, 2004.

Schelling, Thomas C. *The Strategy of Conflict*. 2nd ed., Harvard University Press, 1990.

Schneider, Jacquelyn, Assistant professor in the Strategic and Operational Research Department, U.S. Naval War College; presenting at the Cato Institute “Cyber Warfare, Coercion, and Restraint,” May 9, 2019. https://www.cato.org/events/cyber-warfare-coercion-restraint

Schmidt, Andreas. “The Estonian Cyberattacks” in Jason Healey’s *a Fierce Domain: Conflict in Cyberspace 1986-2012.* Washington DC: Cyber Conflict Studies Association, 2013.

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

Seal, Mark. “An Exclusive Look at Sony’s Hacking Saga.” *Vanity Fair*, February 4, 2015.

Shultz, Colin. “See How Fast ARPANET Spread in Just Eight Years.” *Smithsonian Magazine*. August 28, 2013. Located at: https://www.smithsonianmag.com/smart-news/see-how-fast-arpanet-spread-in-just-eight-years-2341268/ and accessed on February 1, 2021.

Schwartau, Winn. Testimony at Hearing before the Subcommittee on Technology and Competitiveness of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, First Session, June 27, 1991, page 2. Located at: https://winnschwartau.com/wp-content/uploads/2019/06/Testimoney-1991-Computer-security_hearing.pdf and accessed on December 5, 2019.

Sechser, Todd “Goliath’s Curse: Coercive Threats and Asymmetric Power, *International Organization*, Vol. 64, No. 4, (October 2010): 627–60.

Sharp, Travis. “Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony.” *Journal of Strategic Studies,* Vol. 40, No. 7 (2017): 898–926. https://doi.org/10.1080/01402390.2017.1307741

Slayton, Rebecca. “What is the Cyber Offense-Defense Balance?” *International Security* Vol. 41, No. 3 (Winter 2016/2017).

Smeets, Max. “A matter of time: On the transitory nature of cyberweapons.” *Journal of Strategic Studies,* Vol. 41, No. 1–2 (2018):6–32.

Smeets, Max. “The Strategic Promise of Offensive Cyber Operations.” *Strategic Studies Quarterly*, Vol. 12, No. 3 (Fall 2018): 90-113.

Stein, Jeff. "Book review: 'Cyber War' by Richard Clarke." *The Washington Post,* May 23, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/05/21/AR2010052101860.html

Strassler, Robert B. and Richard Crawley. 1998. *The Landmark Thucydides: a Comprehensive Guide to the Peloponnesian War*. New York: Simon & Schuster

Symantec Threat Hunter Team. “FASTCash: How the Lazarus Group is Emptying Millions from ATMs.” *Symantec Enterprise Blog: Threat Intelligence*, November 8, 2018. Located at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware and accessed on December 8, 2019.

Tamkin, Emily. “10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?” *Foreign Policy*, April 27, 2017.

Tapon, Francis. “The Bronze Soldier Explains Why Estonia Prepares For a Russian Cyberattack.” *Forbes,* July 7, 2018. https:// www.forbes.com/sites/francistapon/2018/07/07/the-bronze-soldier-statue-in-tallinn-

estonia-give-baltic-headaches/?sh=59f777da98c7 and accessed on November 14, 2019.

Tassi, Paul. "'The Interview' Made $15M At the Digital Box Office On A $44M Budget." *Forbes,* December 29, 2014.

Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian.* May 16, 2007.

TrendMicro. "Website Defacement." Located at: https://www.trendmicro.com/vinfo/us/security/definition/website-defacement

Tsing, William. "The Advanced Persistent Threat files: Lazarus Group." *MalwareBytes Labs*, March 12, 2019. Located at: https://blog.malwarebytes.com/threat-analysis/2019/03/the-advanced-persistent-threat-files-lazarus-group/ and accessed on January 15, 2021.

United Nations General Assembly: Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. *Final Substantive Report*, March 10, 2021. Located at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

United Nations General Assembly: Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. *Compendium of Statements in Explanation of Position on the Final Report.* March 8-12, 2021. p. 45 Located at: https://undocs.org/pdf?symbol=en/A/AC.290/2021/INF/2

U.S. Senate. "Senate Resolution 187--CONDEMNING VIOLENCE IN ESTONIA AND ATTACKS ON ESTONIA'S EMBASSIES IN 2007 and EXPRESSING SOLIDARITY WITH THE GOVERNMENT AND THE PEOPLE OF ESTONIA." *Congressional Record.* Vol. 153, No. 72 (Thursday, May 3, 2007): S5603-S5604.

Valeriano, Brandon and Ryan Maness. *Cyber War Versus Cyber Realities*. Oxford: Oxford University Press, 2015.

Vanderlee, Kelli. "DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors." *FireEye*, December 17, 2020. Located at: https://www.fireeye.com/blog/products-and-services/2020/12/how-mandiant-tracks-uncategorized-threat-actors.html and accessed on January 15, 2021.

Van Evera, Stephen. *Causes of War: Power and the Roots of International Conflict.* Ithaca, NY: Cornell University Press, 1999.

Van Evera, Stephen. *Guide to the Methods for Student of Political Science*. Ithaca: Cornell University Press, 1997.

Van Evera, Stephen. “Offense, Defense and the Causes of War.” *International Security*, Vol. 22, No. 4, (Spring, 1998): 5-43

Viira, Toomas. “Cyber Attacks Against Estonia - Overview and Conclusions.” *Information Technology in Public Administration of Estonia - Yearbook 2007*. Tallinn, Estonia: Ministry of Economic Affairs and Communications, 2008.

Walt, Stephen. “International Relations: One World, Many Theories.” *Foreign Policy*, Spring 1998.

Waltz, Kenneth. *Theory of International Politics*. New York: Random House, 1979.

Wolf, Jim. “U.S. Draws Attention to Information Warfare Threat.” December 26, 2000. http://www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=004ITd. Accessed March 2, 2016.

Yadron, Danny. “Cyberattack on Sony is Called Sophisticated.” *The Wall Street Journal*, December 7, 2014.

Yamato, Jen and Dominic Patten “ ‘The Interview’ Yanked By Regal, AMC & Other Major Chains.” *Deadline*, December 17, 2014.

Yasmann, Victor. “Russia: Monument Dispute with Estonia Gets Dirty.” *Radio Free Europe*, May 4, 2007. Located at https://www.rferl.org/a/1076297.html and accessed on November 23, 2019.

Zetter, Kim. “Experts are Still Divided on Whether North Korea is Behind the Sony Attack.” *Wired*, December 23, 2014.

Zetter, Kim. “The Sony Hackers Were Causing Mayhem Years Before They Hit the Company.” *Wired*, February 24, 2016.

Zetter, Kim. “Sony Got Hacked Hard: What We Know and Don’t Know So Far.” *Wired*, December 3, 2014. Located at: https://www.wired.com/2014/12/sony-hack-what-we-know/ and accessed December 2, 2019.

CURRICULUM VITAE