THE BIRTH OF A DOMAIN: UNDERSTANDING THE ORIGINS OF FEAR AND OPTIMISM FOR CYBER CONFLICT

by

AARON D. REID

(Under the Direction of Jeffrey Berejikian)

ABSTRACT

Since its creation, the public and policymakers have shared two common perceptions regarding the cyber domain: fear and optimism. Polling reveals that the public fears cyber attacks more than any other form of conflict or crime. Similarly, elites often equate the potential consequences from cyber attacks with established weapons of mass destruction, while also expressing optimism that cyber weapons will shorten wars and spare lives. Increasingly, this combination of fear and optimism is reshaping foreign policy, military strategy, and public morale. The US government's cyber operations budget is now comparable to the US nuclear triad budget. Nuclear budgets grew in response to the overwhelming power the weapons demonstrated in WW2; this type of demonstration event has not occurred in the cyber domain. While cyber threats are increasing, the actual damage they have caused to date is negligible compared to established domains of military conflict. Moreover, cyber attacks have shown little ability to alter the political calculus of a state, meaning optimism about the capacity of cyber to reduce the length of conflicts is unsupported. In this proposal, I offer a framework to explain why the perception of cyber conflict appears disconnected from the historical record and show how this combination of fear and optimism shapes US policy in the domain. My argument relies

upon established concepts in the international relations literature concerning how decision-makers process national security threats. Cyber optimism is rooted in a pervasive belief that cyber offense trumps cyber defense, while cyber fear stems from the inherent difficulty in distinguishing between offensive and defensive cyber operations. In this dissertation, I examine three dimensions of the relationship. First, I evaluate the generalizability of my argument through a comparative analysis of the air domain in the early 20th century and the modern cyber domain. Second, I conduct a survey experiment of 1,000 US residents and a second experiment on 64 cyber experts to test the validity of my theory. Third, I utilize process-tracing to analyze the development of US cyber policy from 1986 to 2014 to show how these causal mechanisms functioned during policy debates.

INDEX WORDS: International relations, cyber, cyberwar, security, domain, survey experiment, fear, optimism, perceptions

THE BIRTH OF A DOMAIN: UNDERSTANDING THE ORIGINS OF FEAR AND OPTIMISM FOR CYBER CONFLICT

by

AARON REID

BS, Middle Tennessee State University, 2002

MS, Embry-Riddle Aeronautical University, 2011

MA, Air Command and Staff College, 2015

MPhil, School of Advanced Air and Space Studies, 2016

A Dissertation Submitted to the Graduate Faculty of The University of Georgia in Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

ATHENS, GEORGIA

2019

THE BIRTH OF A DOMAIN: UNDERSTANDING THE ORIGINS OF FEAR AND OPTIMISM FOR CYBER CONFLICT

by

AARON REID

Major Professor:	Jeffrey Berejikian
Committee:	K. Chad Clay
	Rongbin Han
	Michael Lynch

Electronic Version Approved:

Ron Walcott
Interim Dean of the Graduate School
The University of Georgia
December 2019

DEDICATION

I dedicate this project to my three wonderful kids Austin, Landon, and Emmalyn. They are the light of my life and the sole source of the energy I needed to finish this project. I love you guys with all my heart. You are the reason my heart beats…

ACKNOWLEDGEMENTS

I made my decision to attend the University of Georgia after meeting Dr. Jeff Berejikian while on a campus visit during my school exploration phase. His affable nature, impressive resume, and graceful ability to guide me with my very scrambled idea for a dissertation research question during our first meeting quickly made me realize studying under him at Georgia was the right choice. I would like to thank him for his countless hours of guidance and mentorship as he steered me to a worthwhile project with the skills needed to accomplish it. I was only able to finish this project because of his assistance, wisdom, and patience.

I would also like to thank my committee members: Dr. K. Chad Clay, Dr. Rongbin Han, and Dr. Michael Lynch. I asked them to be on my committee because they were true standouts from their peers. From Dr. Clay I learned that a calm and easy-going demeanor combined with wicked smart intellects is a recipe for widespread acclaim from students and faculty alike. From Dr. Han I learned that an extremely inquisitive mind combined with a gifted ability to communicate complex ideas clearly (in a second language no less) contributes greatly to student success. Dr. Lynch I taught me that there is a way to effectively teach students a subject that they feel will overwhelm them. His ability to explain statistical methods into processes and procedures I could understand and implement increased my confidence in my research abilities. None of these four professors likely realize how much I appreciate their efforts in my journey to join their ranks; I write it here as a permanent record. Thank you.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER 1

INTRODUCTION TO THE RESEARCH QUESTION

The Fear

"Cyberwar is coming!"
John Arquilla and David Ronfeldt – 1993

"[America cannot] wait for the cyber equivalent of the collapse of the World Trade Centers"
Director of National Intelligence Mike McConnell – 2009

"The next Pearl Harbor could very well be a cyber attack"
CIA Director Leon Panetta – 2011

The Optimism

"There were a number of measures that could have been taken sooner and some that were never actually implemented that would have augmented – maybe even been more powerful than – the military instrument, maybe have prevented the use of the military"
NATO Supreme Allied Commander General Wesley Clark suggesting cyber forces may have been able to topple Milosevic without the need for aerial bombing - 1999

"Cyberspace and its associated technologies offer unprecedented opportunities to the United States… [and] by extension, to all aspects of military operations"
Defense Secretary Robert Gates – 2009

"Cyber war skips the battlefield. Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defense."
White House National Coordinator for Security, Infrastructure Protection, and Counterterrorism - Richard Clarke – 2010

Introduction

Data show elites and the public fear adversarial cyber attacks at rates higher than other forms of attack (e.g., terrorism) despite an empirical record that indicates marginal losses for cyber victims. Optimism also abounds regarding the ability for cyber weapons to make future conflict easier for the side that uses them effectively despite limited-to-no battlefield proof of cyber weapon efficacy. This optimism and fear exist without an empirical foundation. Cyber

weapons have shown the ability to inflict some level of harm on society, and there are well-documented instances of hacking, denial of service, identity and intellectually property theft, online espionage, and limited cases of cyber sabotage (e.g., Stuxnet). However, the data show that states, businesses, and the public conduct the vast majority of their online affairs with relatively few problems. Indeed, the average netizen has experienced "no or minimal financial and time losses" due to nefarious cyber activity.[1] There is no record of death from cyber attacks and no record of any cyber attack provoking another state to retaliate with conventional forces. Yet against this backdrop of non-violent and relatively cost-free cyber domain use, there exists a palpable fear of cyber weapons. Further, despite never having proven themselves capable of altering the outcome of a conflict, there exists optimism for cyber weapons to do so in the future.

Public opinion polls indicate citizens fear cyber attacks at higher levels than conventional crimes or weapons (e.g., violent crime, terrorism, nuclear weapons). This fear drives nearly 6 out of 10 Americans to classify cyber attacks on the Department of Defense as an act of war.[2] Elites also display a level of fear that is not commensurate with the level of cyber damage and loss experienced by citizens and states. Many elites believe cyber weapons have "negligible" costs to the attacker, yet they can impose "immeasurable" costs to the victim, even though the empirical record shows otherwise.[3] Some have even predicted that cyber warfare will become a more significant revolution in warfare than gunpowder or the militarization of the air domain.[4] For example, Barack Obama stated in a 2008 campaign speech that nuclear, biological, and

[1] Roberts, Indermaur, and Spiranovic, "Fear of Cyber-Identity Theft and Related Fraudulent Activity," *Psychiatry, Psychology, and Law*, 2013: 315-328.
[2] 60 Minutes / Vanity Fair Public Poll. 2010.
[3] Mazanec, Brian. *"The Evolution of Cyber War: International Norms for Emerging-Technology Weapons"* University of Nebraska Press, Omaha. 2015: 231.
[4] Bender, Jeremy, "Israel: Cyber Is a Bigger Revolution in Warfare Than Gunpowder" *Business Insider*, February 4, 2014, http://www.businessinsider.com/the-internet-is-the-next-battlefield-2014-2 (accessed May 11, 2018).

cyber weapons posed the three greatest threats of the 21st century.[5] Thus far, we have no research that examines and explains why people equate cyber weapons to nuclear and biological weapons when their empirical records of death and destruction are not even remotely similar.

The rapid growth of the cyber domain over the past several decades has caused much disagreement over cyber strategy and policy. Understanding the source of the fear and optimism that drive much of this debate has critical foreign policy implications. The US government's cyber budget has multiplied over the past two decades and is now comparable to the nuclear triad budget. This budgetary shift has occurred while spending has remained relatively level for all other domains. The fear and optimism that shape such policy extend beyond political elites and permeates public preferences as well. Polling indicates cyber threats create more fear among the public than any other threat despite data showing that most citizens have suffered little-to-no losses due to cyber attacks. Current cyber research tends to focus on what role fear and optimism play in cyber policy while mainly ignoring the causal factors for these perceptions.

This project offers a framework to explain the process of perception creation and maintenance for a new domain. Elevated levels of fear result from the inherent difficulty in distinguishing between the offense and defense in the cyber domain. Obscurity between the two forms of war causes fear because people cannot ascertain the purpose of cyber operations. In other military domains, the posture and placement of airplanes, soldiers, and boats help communicate their intended purpose: offense or defense. This demarcation does not exist for cyber attacks; a cyber intrusion by an adversary could be for defensive intelligence gathering, or it could be to plant an offensive virus designed to cripple military command and control networks. The opaqueness of cyber operations and intentions causes fear.

[5] Obama, Barack, "Obama Remarks on Confronting Terrorist Threats" *Washington Post*, July 16, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/07/16/AR2008071601474.html (accessed November 16, 2016).

Optimism results from the widely held belief that cyber offense trumps cyber defense. Unlike soldiers, boats, and aircraft that decision-makers can deploy defensively to blunt an impending attack, the cyber domain requires a defense that is everywhere at all times. There is nothing to deploy against impending cyber attacks, nor is there generally any warning that a cyber attack is imminent. Instead, cyber defense needs to exist everywhere and at all times. Strong cyber defenses have proven difficult, however, as successful cyber attacks occur continually. This combination causes a pervasive belief in the efficacy of cyber offense over cyber defense, and fuels cyber optimism even in light of weak empirical evidence to support such a perception.

I validate the generalizability of my theory by showing my theoretical tenets worked in a nearly identical fashion during the exploitation of the air domain in the early 20th century. Understanding the origins of these perceptions is vital given the shifts in defense postures we see in response to cyber threats, the preeminence of fear in world politics, and the political pressure created by heightened public fear of a given threat.

The Puzzle

Why do we observe optimism for cyber weapons to alter the political calculus of an enemy during a conflict? Why do people fear cyber attacks at a level disproportionate to the damage they cause? There is no obvious source for this optimism and fear because the empirical record shows no cyber weapon has ever killed a person or caused widespread or lasting damage to societies. There have also been no cyber demonstration events (e.g., a 'cyber' Pearl Harbor) that would provide the foundations for these perceptions. If we do not have the cyber equivalent of Hiroshima or Nagasaki to ground these fears, what then explains the creation and maintenance of these beliefs? Biological and chemical weapons proved their lethality in both WW1 and

WW2, and thus there is a natural connection between public fear and the weapon's record of destruction. Nuclear weapons proved their destructive capability in WW2 and tested explosions from the 1940s and beyond.

Cyber attack data, however, show they are responsible for no deaths, little to no destruction, and negligible losses for citizens and states. Nevertheless, we find both elites and the public are optimistic that the cyber domain can tilt a future conflict in their state's favor, and they fear adversarial cyber attacks at levels commensurate with traditional weapons of mass destruction. To frame the puzzle, I first assess fear and optimism for the cyber domain among the public and elites. Next, I summarize cyber weapon development and use from the 1980s until the present to capture the losses sustained by individuals and states from cyber weapons. Juxtaposing the empirical record with the beliefs and preferences held by the public and political leaders highlights a disconnect between cyber reality and cyber rhetoric.

Cyber Fear

There is an intense fear among elites and the public regarding adversarial cyber attacks. The result of this fear is hyperbole and rhetoric not grounded in data or any real-life demonstration event. Making such claims without an empirical foundation has vast policy implications for powerful states. For example, in 2007, Director of National Intelligence (DNI) Mike McConnell briefed President Bush on a hypothetical scenario: instead of terrorists flying aircraft into buildings on 9/11, they simply broke into the computer databases of several major financial organizations and erased the contents. McConnell told the president that erasing or corrupting just a portion of the information would cause mass panic and entire economies to collapse for lack of confidence in financial transactions. "The economic effects of this attack,"

McConnell told the president, "would be worse than those of the physical attacks of 9/11."[6] Bush responded by telling McConnell and that he wanted the US to undertake a cyber version of the Manhattan Project, alluding to the secret and costly WW2 project that built the atom bomb. The meeting resulted in a proposed 5-year $40 billion project that sought to expand US cyber capabilities vastly.[7]

Only a few years later, Michael Hayden, who served as director of both the CIA and NSA, stated that powerful cyber weapons were "a new class of weapon, a weapon never before used" that hinted at a "whiff of August, 1945."[8] Just as Obama did in 2008 and many other political elites have done elsewhere, Hayden compared cyber weapons, which have zero attributed deaths and scant physical destruction on their resume, to that of nuclear weapons This is puzzling because nuclear weapons have killed hundreds of thousands of people and caused untold destruction.

Fear of cyber weapons extends beyond political elites. Public polling conducted between 2013 and 2016 shows 70 percent of Americans believe cyber attacks pose a significant threat to the well being of the US, 57 percent believe cyber attacks aimed at the Pentagon should be considered an act of war, and 62 percent believe the US is not prepared for a significant cyber attack.[9] Gallup polling from 2017 found that the crime Americans feared the most was losing their personal information to cyber hackers (67 percent worried about it) while being a victim of identity theft came in second with 66 percent. The next highest crime worry was auto theft at 38

[6] Harris, Shane. 2014: 142.
[7] Harris, Shane. 2014: 143.
[8] Seabrook, "Network Insecurity," *The New Yorker*, 20 May 2013: 70.
[9] Roper Center. *iPOLL Search Results.* 2013 - 2016. http://ropercenter.cornell.edu/CFIDE/cf/action/ipoll/ipollResult.cfm?keyword=cyber+attacks&exclude=&topic=Any&organization=Any&fromDate=&toDate=&questionViewId=&label=&studyId=&sortBy=BEG_DATE_DESC&search=submit (accessed February, 2016).

percent, while terrorism came in at 30 percent, robbery at 25 percent, and sexual assault at 18 percent.[10]

Unfortunately, public polling conducted thus far on cyber threats is vastly inadequate for the intricacies of the cyber domain and gives us little information other than to tell us that the public genuinely fears cyber weapons. As an example, a review of numerous public polls on Cornell's Roper Center website showed all polling data related to cyber attacks posed questions such as "Do you consider cyber attacks an act of war?" The problem with asking for opinions about 'cyber attacks' is that 'cyber attack' is a generic term that conveys no sense of scale or destructive potential. This question is akin to asking the public if they believe "a weapon attack" is an act of war. Without knowing whether the weapon is a pocketknife or a nuclear missile, there is little useful information that researchers or decision-makers can glean from the data.

These data, however, only tell us there is outsized fear among the public for the two most common forms of cyber attacks that pose a threat to the average citizen: identity theft and loss of personal information from cyber attacks. The polling results give us no insight as to why the public fear these events at such high levels and only serve to frame the research question, not answer it. A common explanation for these high fear numbers is that the fear is warranted because so many Americans are subject to identify theft and loss of personal information. An in-depth examination of the data, however, shows that the rate at which individuals are subject to these forms of cyber attacks does little to explain this fear.

Cyber attacks against individuals do appear to affect a rather large portion of society when compared to other types of crime, yet their dollar cost and personal impact is rather low in comparison. In 2014, approximately 17.6 million US residents were victims of cyber identity

[10] Reinhart, RJ. "Cybercrime Tops Americans' Crime Worries." *Gallup*. November 6, 2017. http://news.gallup.com/poll/221270/cybercrime-tops-americans-crime-worries.aspx (accessed May 24, 2018).

theft, with an estimated cost of $15.4 billion.[11] By comparison, in 2014, there were 1.16 million violent crimes and 8.27 million property crimes reported for a total cost of $14.3 billion.[12] However, the US Department of Justice (DOJ) reports that of the 17.6 million identity theft victims, only 14 percent (2.5 million) had out-of-pocket losses that exceeded $1, and only half of those people (1.25 million) suffered a financial loss over $100.[13] When we juxtapose these findings, we see that there are nearly as many victims of violent crimes every year in the US (1.16 million people) as there are victims of cyber attacks that cause a loss of $100 or more (1.25 million people).

In short, the average American in 2014 was nearly as likely to be a victim of rape, murder, armed robbery, or another violent crime as they were to be a victim of a cyber attack that caused more than $100 in out-of-pocket expenses. Despite this, 2014 Gallup polling shows people fear cyber attacks at rates roughly three times higher than they fear violent crimes and terrorism. The data also reveals another interesting finding: the DOJ reported in 2010 that there were 8.6 million victims of identity theft, which is roughly half as many as in 2014.[14] Yet Gallup polling from 2010 showed Americans feared identity theft at a rate of 70 percent. This 2010 'cyber fear' percentage is four points higher than in 2014 when there were nearly twice as many reported cases of identity theft than in 2010.[15] The disparity indicates that it is not necessarily the number of cyber attacks against citizens that are causing cyber fear, nor is it the

[11] Harrell, Erika. "Victims of Identity Theft, 2014." *U.S. Department of Justice, Bureau of Justice Statistics.* November 13, 2017. https://www.bjs.gov/content/pub/pdf/vit14.pdf (accessed May 25, 2018).
[12] Federal Bureau of Investigation, "FBI Releases 2014 Crime Statistics." *FBI.gov*. September 28, 2015. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2014-crime-statistics (accessed 26 May 2018).
[13] Harrell, Erika. 2014: 1-7.
[14] Langton, Lynn. "Identity Theft Reported by Households, 2005-2010." *U.S. Department of Justice, Bureau of Justice Statistics.* November 2011. https://www.bjs.gov/content/pub/pdf/itrh0510.pdf (accessed May 25, 2018).
[15] Gallup Polling. "Crime Fear Summary 2005 - 2010." *Gallup*. nd. http://news.gallup.com/poll/1603/crime.aspx (accessed May 27, 2018).

damage they caused. Instead, there is another causal mechanism creating and sustaining fear and optimism that is unexplored by researchers.

While nefarious cyber activity affects all people in some way, the aggregate metrics of cyber losses individually and globally do not appear substantial enough to support the rhetoric that many people espouse or the elevated levels of fear regarding the capability of the cyber domain. The purpose of this research project is not to quantify whether cyber weapons are or are not powerful weapons that people are rightful to fear. Nor is my goal to determine if cyber weapons will shorten future wars, reduce combat causalities, rectify asymmetric power balances between states, or prove capable of crippling a society. Instead, I seek to understand *why* and *how* these fears and perceptions formed for the cyber domain given the lack of empirical evidence to support them.

Cyber Optimism

Many scholars and elites believe the cyber domain offers the ability to bypass conventional battlefields and render enemy forces powerless during a cyber onslaught. Peterson (2013) theorizes states will use cyber weapons as a strategic enabler by attacking software systems that control electric grids, power production facilities, refineries and pipelines, and transportation networks.[16] As an example, the attacking force could use cyber operations to shut down a power production facility and water treatment plant in a particular area before a conventional kinetic attack. The shutdown may cause civilians to leave the affected towns and allow the attacking state increased flexibility and efficiency when targeting enemy forces. The cyber attacks alone may also reduce the need for costly strategic bombing campaigns against infrastructure. Peterson's target selection for cyber weapons is not unlike that of early airpower

[16] Peterson, Dale. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies,* 2013: 120-124.

theorists who believed attacking enemy infrastructure and production facilities were vital to choking out the enemy (e.g., Allied air strategy in WW2).

Whereas many authors theorize about what a state *could* do with the cyber domain during a conflict, Arquilla (2012) asserts that cyberwar is already underway. The goal, Arquilla says, is less about defeating an adversary's military and more about the ability to attack a nation's infrastructure without having to fight a conventional war first.[17] This theory parallels work by early airpower theorists like Mitchell (1925) and Douhet (1921), who wrote extensively about the airplane's ability to overfly land and sea forces to attack enemy infrastructure. More recently, renowned scholars like Nye (2011) have asserted that cyberwar could "have effects that amplify or are equivalent to major kinetic violence."[18] Military strategists from many states have similarly concluded that cyber weapons are viable tools against conventional forces.

These beliefs mirror, nearly precisely, the perceptions held by the public and elites after the invention of powered flight and the militarization of the air domain in the early 20th century. In the case of early airpower, civilians and elites expected airpower to win future wars for their nation, and they feared adversarial aerial attacks. Both of these perceptions existed before aircraft proved themselves capable of inflicting meaningful destruction in warfare.

Initially, states utilized early aircraft in combat to surveil enemy troop positions and movements to improve their odds. During the first weeks of World War 1, pilots proved themselves useful only as information gatherers. The intelligence gleaned by aviators in the early portion of the war "played a significant role" in the German destruction of the Russian Second Army at Tannenberg in August 1914.[19] Many of these sorties were scouting missions designed to gather intelligence that would bolster an army's defensive posture. In short order,

[17] Arquilla, John. "Cyber War is Already Upon Us." *Foreign Policy,* March/April 2012.
[18] Nye, Joseph Jr. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly.* Winter, 2011: 21.
[19] Kennett, Lee. *The First Air War – 1914 - 1918.* New York. Simon and Schuster, 1991: 31.

however, technological developments allowed militaries to lade their aircraft with munitions and guns. By 1917, aircraft were attacking cities with small munitions with "almost commonplace occurrence."[20]

As with cyber today, data show that the fear and optimism for early airpower was unfounded. A report of French and British aerial bombing efforts in 1915 showed that of 141 attempts to bomb enemy railway stations, only 3 (2.1 percent) produced weapon impacts close enough to be called useful.[21] Even the effective attacks, however, were more symbolic because the munitions dropped at the time had limited destructive potential. Historical analysis shows that "strategic aviation in fact played little role in the 1914-1918 conflict."[22] Despite this, citizens and elites displayed vast optimism and fear for the airplane to alter conflicts dramatically. For example, Thomas Edison stated in 1921 that the airplane could destroy a large city in five minutes despite having never proven its ability to inflict even moderate damage to small cities.[23] Even with no demonstration event to ground this airpower rhetoric, however, scholars, elites, and laypeople alike bought into the notion that the airplane was "the offensive weapon par excellence" during the early days of airpower.[24] Just as with cyber weapons today, data or real-life performance did not create or sustain optimism and fear of the early aircraft. Today, this same process is occurring as we see unfounded fear and optimism pervading all strata of political and military thought regarding cyber weapons.

As an example, the People's Liberation Army (PLA) of China made the rare move of publishing a military tactics book written by two senior PLA Colonels. In the 1999 book,

[20] Kennett, Lee. 1991: 55.
[21] Kennett, Lee. 1991: 51.
[22] Morrow, John. "The First World War, 1914-1918, in *A History of Air Warfare*. by John Olsen, 3-26, Potomac Books, Dulles VA. 2010:24.
[23] Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing.* Princeton University Press, New Jersey. 2002: 148.
[24] Douhet, Giulio. 1921/2009: 15.

Colonels Qiao Liang and Wang Xiangsui theorize about the best military strategies for developing states to use against a great power. After proposing various asymmetric tactics to employ against the US specifically, the authors describe how cyber weapons will influence future conflict. They write:

> If the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and political crisis.[25]

The Colonels' expectation for the cyber domain to alter future conflict in a fundamental manner is similar to optimism for airpower in the early 20th century. In his widely read 1921 book *The Command of the Air*, Italian soldier and air power theorist Giulio Douhet wrote:

> By bombing railroad junctions and depots, population centers at road junctions, military depots, and other vital objectives, Air Force A could handicap the mobilization of B's army. By bombing naval bases, arsenals, oil stores, battleships at anchor, and mercantile ports, it could prevent the efficient operation of B's navy. By bombing the most vital civilian centers it could spread terror through the nation and quickly break down B's material and moral resistance.[26]

For both the air and cyber domain, military strategists had/have expectations for the new domain of their day to 'overfly' the battlefield and craft a quick end to the conflict. Also similar for both cases is that the strategists made these conjectures without any evidence that the new domain could inflict the expected damage on society. This cyber optimism is rooted in the belief, succinctly stated by Stone (2013), that "a few keystrokes are all that are required to set in train a sequence of potentially very violent acts."[27] Interestingly, the preceding summary of

[25] Liang Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999: 145-146.
[26] Douhet, Giulio. 1921/2009: 57.
[27] Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies*, 2013: 107.

major cyber attacks showed there is little-to-no evidence to support such beliefs. Such a disconnect mirrors the problem with perceptions for early airpower: for much of the early 20th century, there was little evidence that the airplane could inflict the damage airpower theorists believed it could, yet elites continued to construct policies based on these perceptions.

The preceding summary of cyber optimism and fear shows that both perceptions exist at high levels among the public and policymakers. Next, I assess the damage caused by cyber attacks for individuals, corporations, and states.

Cyber Reality

States, corporations, and individuals employ cyber attacks for a host of different objectives. To capture the broad nature of cyber attack reality accurately since the 1980s, I separate their use into military and civilian categories. Military cyber attacks during the dawn of the cyber age generally centered on covert forms of espionage. In what is one of the first reported cyber espionage events, a team of German hackers stole information related to President Reagan's Strategic Defense Initiative (SDI - i.e., Star Wars) from several US research facilities in 1986. The objective of the attack, known as Cuckoo's Egg, was to find information that Russian spies would be willing to buy. American officials eventually arrested the hackers and sentenced them to prison. The attack, however, did little to spur organizational or policy change within the burgeoning global cyber enterprise and had no meaningful impact on the SDI program.[28]

In February 1998, a major cyber attack, code-named Solar Sunrise, compromised hundreds of computers and networks at multiple military and government research locations. The three-week-long attack started shortly after tensions escalated in the Middle East in early 1998. In January 1998, Iraq barred United Nations (UN) nuclear inspectors from accessing

[28] Healey, Jason. "*A Fierce Domain: Conflict in Cyberspace, 1986 to 2012."* CCSA, USA. 2013:31

several military sites. President Clinton responded in February by sending several thousand additional combat troops to the region. Solar Sunrise coincided with these developments, and government officials described the attack as "the most serious intrusion into the United States up to that point."[29] With the attacks happening against the backdrop of growing US/Iraq tensions, Deputy Defense Secretary Hamre briefed President Clinton that "the [cyber] intrusions might be the first shots of a genuine cyber war, perhaps by Iraq."[30] Tensions began to subside in late February when intensive diplomatic negotiations resulted in a UN Memorandum of Understanding that Iraqi leaders agreed to sign. Several weeks later, US investigators discovered the identity of the Solar Sunrise hackers: two 16-year-olds from Northern California and an 18-year-old living in Israel. The hackers later told investigators they initiated the attack for fun.

One of the first examples of a state-sponsored hacking event is the 1998 Moonlight Maze cyber attack. During the attack, Russian hackers, some operating out of the Russian Academy of Sciences, broke into "hundreds of computers at NASA, the Pentagon, and other government agencies, as well as private universities and research laboratories."[31] The hackers stole unclassified but sensitive information on US defense research projects. Despite the losses, US officials reacted by only sending a formal demarche to the Russian government. Reports state the Russians mostly ignored the demarche.[32] The only internal changes the US made in response to the attack was to reroute unclassified internet traffic through government monitored gateways that could detect future attacks quicker, along with an order for all DoD personnel to change their computer password.

---

[29] Healey, Jason. 2013: 122.
[30] Graham, Bradley. *U.S. Studies a New Threat: Cyber Attack.* Washington Post, May 24, 1998. http://www.washingtonpost.com/wp-srv/washtech/daily/may98/cyberattack052498.htm (accessed May 12, 2018).
[31] Money, Art. "*Cyber security "Wake-Up" Calls for the Federal Government,"* no date. CTOVision. https://ctovision.com/cyber-security-wake-up-calls-for-the-federal-government/ (accessed May 12, 2018).
[32] Healey, Jason. 2013: 49.

The next major state-sponsored cyber attack began in the late 1990s when the Chinese government began a broad espionage program against multiple US government organizations. During the multiyear event, Chinese hackers allegedly broke into US government computer systems at the DOD, Department of Homeland Security (DHS), State Department, Department of Energy (DOE), and various defense contractors. Reports also emerged alleging intrusions into the offices of the Dalai Lama, embassies from multiple states, and German chancellor Angela Merkel's personal office computer.[33] During the campaign, the hackers downloaded over 50 terabytes worth of US defense data, including blueprints for the new F-35 fighter jet. While the cost of this operation appears to be quite high for the victims, the Wall Street Journal reported in 2013 that the US government chose to respond to the multiyear cyber campaign by only issuing a one-page formal demarche to the Chinese government.[34]

Russian hacking activity in Estonia in 2007 and Georgia in 2008 represents one of the first non-espionage uses of cyber weapons. Russia conducted the attacks because local Estonian officials sought to remove a statue of a Soviet soldier. Russian officials and nationalists became incensed at the efforts to remove the statue and conducted Distributed Denial of Service (DDoS) attacks aimed at Estonian government websites, financial institutions, and national internet connection points. Although the attacks continued for several weeks during April and May of 2007, computer technicians restored much of the necessary services quickly to citizens and the government. In the end, Estonian officials moved the statue, and experts consider this a "tactical and strategic defeat" for Russian cyber forces.[35]

[33] Healey, Jason. 2013:69.
[34] Gorman, Siobhan. *Wall Street Journal.* April 22, 2013. http://www.wsj.com/articles/SB10001424127887324345804578424741315433114 (accessed December 2, 2016)
[35] Healey, Jason. 2013: 70.

Russian cyber attacks on Georgia the following year coincided with a dispute over the breakaway region of South Ossetia. Russian DDoS attacks took several important Georgian websites offline, including that of the parliament and several news agencies. The Russian government also undertook kinetic military action during this period, marking what may be the first coordinated conventional/cyber military operation. Despite some successes for the Russians during the attacks, the overall impact of the cyber campaign was "rather minor" because Georgia had few vital services tied to the internet.[36] The effect for Georgian citizens was a stop on electronic banking services for approximately ten days until technicians restored full service.

One of the most widespread DOD computer virus attacks also occurred in 2008. The attack started when an unknown (though presumably Russian based on forensic analysis) foreign intelligence service left an infected USB thumb drive outside of a US military base in the Middle East. An unwitting US service member inserted the USB drive into a government computer, which allowed the virus to access to US computer systems. To the surprise of US cyber experts, the virus was not contained only to the DOD's unclassified network where the virus started but also had spread to air-gapped Secret and Top Secret computer systems.[37] After over a year of work and the theft of untold amounts of sensitive data, technicians eradicated the virus. The event garnered attention from the highest levels of the US government and eventually became the catalyst for the creation of a single military entity to oversee all US cyber defense operations: the US Cyber Command.[38]

The Stuxnet attack of the early 2010s is one of the only cyber events that caused physical damage for the victim. The attack, purported orchestrated by the US and Israel, was part of an extensive covert operation designed to delay and deter the Iranian government from developing

[36] Rid, Thomas. 2013: 8
[37] Healey, Jason. 2013: 73.
[38] Harris, Shane. 2014: 150.

nuclear weapons. The Stuxnet virus began surgically infecting Iranian computer systems at the Natanz nuclear plant sometime around 2010. The virus rapidly altered the speed of Iranian P-1 nuclear enrichment centrifuges and caused premature failure of the components. At the same time, the virus altered display information to local plant technicians to mask the centrifuge oscillations. The goal of the attack was to slow down Iranian enrichment by causing premature failure of the centrifuges with the hope that local Iranian technicians would struggle to fix what appeared to be typical industrial component failures.[39] The result of the attack is debatable.

Kaspersky Labs, a well-known computer security corporation, suggested that the Stuxnet attack set Iranian nuclear efforts back by five years.[40] The US intelligence community estimated the attack cost Iran approximately two years,[41] while the International Atomic Energy Association (IAEA) suggested that the attack cost Iran no time because they sped up production on uninfected centrifuges.[42] Others have also suggested that the attack may have helped the Iranians because it spurred them to replace the aging P-1 centrifuge with more reliable components (North Korea and Pakistan had both previously deemed the notoriously unreliable P-1 unfit for their nuclear programs).[43] Beyond the rather minor physical damage the Stuxnet attack caused, Rid (2013) believes the Stuxnet attack sent a nearly worthless political message to the Iranians in the high-stakes game of nuclear non-proliferation: "*we're alert and technically sophisticated, but we're not really serious about attacking you if you cross a red line."*[44] (emphasis in original)

[39] Valeriano, Brandon and Ryan Maness. 2015: 152.
[40] Barsashka, Ivanka. 2013. "Are Cyber Weapons Effective?" *The RUSI Journal* 158: 49.
[41] Sanger, David. 2012b. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* Random House, New York. 206.
[42] Sanger, David. 2012b: 206.
[43] Sanger, David. *The Reckoning: How President Obama Has Changed the Force of American Power.* Crown Publishing, New York. 2012a: 188.
[44] Rid, Thomas. 2013: 172 emphasis in original.

The striking aspect of the debate over the effects of Stuxnet is that after news broke of the attack, experts heralded it as "the cyber equivalent of dropping the atom bomb"[45] and a "new era in warfare."[46] However, even this advanced cyber attack gave no clear indication as to its usefulness or efficacy in international relations, and it gave no guidepost as to whether states should fear or scoff such attacks. What we find from all of the significant military-centric cyber attacks reviewed is that they had caused little or no political change in the victim's government, caused no deaths, and generated negligible or no physical damage.

An examination of cyber attacks against citizens and corporations also displays a pattern of limited utility for those employing cyber attacks. The primary objective of these attacks is intellectual property or identity theft. According to a June 2014 report co-authored by the Center for Strategic and International Studies (CSIS) and Mcafee Inc., the loss of personal information and intellectual property costs the global economy between $375 billion and $575 billion annually.[47] The CIA's 2014 World Factbook estimates the value of the global economy at $107.5 trillion in terms of purchasing power parity and $78.3 trillion in nominal terms.[48] The cyber losses calculated by CSIS and Mcafee Inc are between .3 percent and .7 percent of the global economy. Such a loss is relatively minor when we consider the increased efficiency that the cyber domain brings to the global economy. Data show relatively little damage or loss at the domestic level as well.

The US Department of Commerce estimates that cyber theft of intellectual property costs the US between $200 billion and $250 billion annually, along with the loss of hundreds of

[45] Broad, William, John Markoff, and David Sanger. "Israel Tests on Work Called Crucial in Iran Nuclear Delay." *NY Times* (NY Times), 15 January 2011.
[46] Clayton, Mark. "The New Cyber Arms Race." *Christian Science Monitor*, 7 March 2011.
[47] CSIS-Mcafee. *Net Losses: Estimated the Global Cost of Cybercrime.* Annual Report, Washington DC: Center for Strategic and International Studies, 2014: 3.
[48] Central Intelligence Agency. *World - CIA World Factbook*. October 6, 2015. https://www.cia.gov/library/publications/download/download-2014/index.html (accessed May 22, 2018).

thousands of jobs.[49] The cost of the malicious cyber activity is widely debated however, with the White House saying in 2018 that *all* cyber attacks cost the US between $57 billion and $109 billion in 2016.[50] This loss seems negligible considering that just the communication and information sector in the US added over $950 billion to the US economy in 2014.[51] The $950 billion figure does not include the added efficiency that the cyber domain brings to all other sectors of the economy, nor does it capture efficiency benefits like online banking and e-commerce.

Findings published in 2016 by RAND researcher Sasha Romanosky suggests that these loss figures from the White House and Department of Commerce are vastly inflated. The researcher shows that cyber attacks only cost US businesses approximately $8.5 billion annually. Romanosky analyzed over 12,000 cyber incidents between 2004 and 2015 and found that "the typical cost of a data breach [for a business] is less than $200,000, far lower than the millions of dollars often cited in surveys (e.g., Ponemon 2015). Moreover, we find that cyber incidents cost firms only 0.4% of their annual revenues, much lower than retail shrinkage (1.3%), online fraud (0.9%), and overall rates of corruption, financial misstatements, and billing fraud (5%)."[52]

An analysis of consumer-focused cyber attacks like that conducted against credit agency Equifax in 2017 also shows relatively little cost imposed on societies. Thus far, the only reported losses from the 2017 Equifax breach, in which nearly 150 million Americans had their credit bureau information stolen, is a 15 percent increase in credit card fraud shortly after the

[49] US Department of Commerce. *Stolen IP Harms American Businesses.* November 29, 2011. http://2010-2014.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businesses-says-acting-deputy-secretary-.html (accessed December 1, 2016)
[50] Hagan, Shelly. "Cyber Hacks Cost up to $109 Billion in 2016, U.S. Estimates." *Bloomberg.* February 16, 2018. https://www.bloomberg.com/news/articles/2018-02-16/cyber-hacks-cost-as-much-as-109-billion-in-2016-u-s-estimates (accessed May 16, 2018).
[51] Bedard, Mathieu. "The Underestimated Economic Benefits of the Internet." *MEI.* March 31, 2016. https://www.iedm.org/59576-the-underestimated-economic-benefits-of-the-internet (accessed May 17, 2018).
[52] Romanosky, Sasha. "Examining the Costs and Causes of Cyber Incidents." *Journal of Cybersecurity.* 2016: 122.

attack and before credit agencies began freezing accounts.[53] Research into other consumer-focused cyber data thefts shows similar results. For example, the 2005 hack of 163,000 customer records stored by ChoicePoint data aggregator resulted in only 800 cases of identity theft, and the 2008 hack of 4.2 million credit and debit card numbers from Hannaford Bros. supermarket chain resulted in only 1,800 cases of fraud.[54] Just as my earlier analysis showed that cyber attacks against militaries and governments have cause little damage and caused few if any political changes, so to have corporate and consumer-centric cyber attacks imposed little cost on businesses and individuals. Despite this, people in all strata of society hold much optimism and fear for cyber attacks.

Understanding the source of cyber optimism and fear is critical to understanding how and why the cyber domain affects domestic and international politics. As I show below, debates about various aspects of the cyber domain are ongoing among researchers without an understanding of why these perceptions exist. Given that optimism for a weapon to make war quick and decisive is a catalyst for conflict (Blainey 1988) and that fear has been a fundamental tenet of international relations from Thucydides to modern times (Bull 1977; Waltz 1959; Schelling 1966), determining the source of cyber optimism and fear deserves scientific attention.

What We Know

Thus far, researchers have only provided tangentially related clues as to why elites and the public fear cyber attacks despite 40 years of history where "no cyber offense has ever caused the loss of human life… ever injured a person… [or] ever seriously damaged a building."[55] The explanations offered by researchers generally center around three key points. First, a lack of

[53] Fickenscher, Lisa. "Credit Card Fraud Spikes After Equifax Cyber-Attack." *NY Post*, September 9, 2017. https://nypost.com/2017/09/08/credit-card-fraud-spikes-after-equifax-cyber-attack/ (accessed May 24, 2018).
[54] Libicki, Martin. *Cyberdeterrence and Cyberwar*. RAND Corporation, Santa Monica CA. 2009: 93.
[55] Rid, Thomas. 2013: 166.

understanding of the domain by elites causes them to focus on what is technically possible rather than on what is realistically feasible. Second, the scarcity of reliable cyber data precludes the production of convincing scientific findings that may restrain heightened levels of cyber optimism and fear. Third, cyber optimism and fear are rightful byproducts of the latent power of cyber weapons. The findings associated with each of these veins, however, do not provide an acceptable answer to the research question. Explaining why political elites have equated cyber attacks to Pearl Harbor, the terrorist attacks of 9/11, and even nuclear attacks against the backdrop of a relatively clean empirical record of cyber 'destruction' requires a focused scientific effort that scholars have not offered thus far.[56]

While the literature gives no direct answer to the research question, some researchers assert that cyber fear results from experts overhyping the dangers associated with cyber attacks. According to researchers who embrace this position, scholars and elites who propagandize cyber's ability to shorten future conflict, cripple societies, and create mass strategic instability in the international system (see Clarke and Knake 2010 and Kello 2013) are causing unjustified inflation of fear and expectations. Scholars believe this occurs because of a lack of understanding of the domain and its technical nature among elites (Walt 2010) or the inability to attribute attacks accurately to a given state or entity (Clark and Landau 2010). The lack of understanding helps foster the impression among elites and the public that cyber attacks occur with near impunity. The result is 'experts' who overhype the threat of cyber weapons, which in turn causes unnecessary fear and unrealistic expectations.

The result of this is the inability to create effective policies for the cyber domain. Research by Cavelty (2007) into cyber terrorism finds that "experts are unable to conclude whether cyber-terror is fact or fiction, or, since they are unwilling to dismiss the threat

[56] Healey, Jason. "*A Fierce Domain: Conflict in Cyberspace, 1986 to 2012."* CCSA, USA. 2013:13

completely, how long it is likely to remain fiction."[57] As a result, policymakers must "navigate the rocky shoals between hysterical doomsday scenarios and uniformed complacency" when trying to create sound public policy.[58] Becoming informed, however, requires data. Gathering the required data that Cavelty says experts need to surmise the damage caused by cyber terrorism is a daunting task. Indeed, noted Harvard law professor Jack Goldsmith stated in 2012, "There is a worry [among political scientists] that writings in this area will have a dearth of relevant data and will not be valued."[59] To Goldsmith's concern, there is only one publically available dataset on cyber attacks: the Dyadic Cyber Incident and Dispute (DCID) dataset published by Valeriano and Maness. The DCID contains 192 cyber incidents between rivals from 2001 to 2011.

Valeriano and Maness (2015) use their dataset to reach conclusions similar to Cavelty. The authors find that only 15.8 percent of rivals engaged in cyber conflict with each other from 2001 to 2011.[60] Because this rate falls below Finnemore and Sikkink's (1998) proposed threshold for what constitutes an international norm (i.e., 1/3 of states follow a given behavioral pattern), they conclude that norms exist that preclude widespread use of cyber weapons. Much like Cavelty, they believe that experts are overhyping the threat cyber attacks pose. The authors, however, do not offer any theory or evidence to explain why experts are overhyping cyber attacks, nor do they explain why the public and elites buy into such rhetoric.

Quigley, Burns, and Stallard (2015) find that the source of cyber optimism and fear are experts who use language that "manipulate[s] common cognitive limitations in order to over-

[57] Cavelty, Myriam. "Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology and Politics,* 2007: 20.
[58] Cavelty, Myriam. 2007: 31.
[59] Interview with Jack Goldsmith. Conducted by Lucas Kello, Cambridge Massachusetts, September 13, 2012.
[60] Valeriano, Brandon, and Ryan Maness. *Cyber War Versus Cyber Realities.* New York, NY: Oxford University Press. 2015: 105.

dramatize and over-simplify cybersecurity risks to critical infrastructure."[61] Their research focuses on the process that occurs when experts use specific language when discussing cyber threats and how cognitive processes translate this language into a threat for the audience. However, their research fails to consider why this process has been so effective given the lack of a cyber demonstration event or empirical evidence to support the rhetoric. Further, they do not identify any specific aspects of the cyber domain that may make this rhetoric more or less powerful (e.g., whether the technical nature of the domain influences the process). In either case, their work parallels other literature that intimates cyber optimism and fear are the results of overblown rhetoric from technical experts and political elites (Gartzke 2013; Rid 2012; Libicki 2011).

In one of the few scholarly works that examine *why* experts and elites would want to overhype cyber threats, Rid (2013) believes the causal mechanism for cyber rhetoric stems from a misunderstanding of what a weapon in war is supposed to accomplish. According to Rid, the weapon must be "instrumental, political, and potentially lethal, whether in cyberspace or not… [and] no stand-alone cyber offense on record meets these criteria."[62] Ride bases this Clausewitzian notion of what constitutes an act of war on the requirement for a weapon to alter the political calculus of another state. Rid's research, along with that of Gartzke (2013) and Libicki (2014), shows that cyber weapons are ineffective because they have demonstrated limited-to-no ability to alter the political calculus of state leaders.

Many researchers aver that elites and experts have overhyped the capabilities and destructive potential of cyber weapons, yet this gives no scientific insight into processes at work

[61] Quigley, Kevin, Calvin Burns, and Kristen Stallard. "Cyber Gurus: A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection." *Government Information Quarterly*, 2015: 108.
[62] Rid, Thomas. 2013: 37.

and provides us with only the most superficial of answers for an issue that influences foreign policy, state relations and perhaps future conflict behavior. While many of these scholars offer a basic explanation for why we should not fear cyber weapons, they do not provide any substantive explanation for why so many experts, decision-makers, and average citizens continue to do so.

A more fundamental problem with this argument is that rhetoric espoused by experts about other weapons or forms of warfare has not caused the same optimism or fear. For example, the terror attacks of 9/11 killed over 3,000 people and caused estimated economic losses of $2 trillion[63] to $3.3 trillion.[64] The rhetoric from experts about terrorism in the post-9/11 environment dominated the daily news cycle and was at least equal, if not greater, than any hype about cyber weapons since then. Despite this increase in daily rhetoric, Gallup polling shows fear of terrorism among the US public maxed out at 47 percent after the 9/11 attacks and has since settled to the 30-40 percent range, while fear of cyber attacks remained consistent around 70 percent.[65] Thus, 'expert rhetoric' did not operate in the same fashion for terrorism as some researchers postulate it does for cyber threats. Theories that pin the cause of cyber optimism and fear on 'expert hyperbole' do not address this issue, and this serves to reinforce my claim that the causal mechanisms that create and sustain cyber fear and optimism are still undefined in cyber literature.

The last strand of cyber research that broaches the research question posits that cyber optimism and fear are rational, given the prior use of cyber weapons. Generally, researchers who advocate for this theory believe that the interconnectedness of people, businesses, and

---

[63] Institute for the Analysis of Global Security. *How much did the September 11 Terrorist Attack Cost America?* http://www.iags.org/costof911.html (accessed May 23, 2018).
[64] New York Times. *One 9/11 Tally: $3.3 Trillion.* https://archive.nytimes.com/www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=1 (accessed May 23, 2018).
[65] McCarthy, Justin. "Americans' Worries About Most Crimes Similar to 2015." *Gallup*. November 14, 2016. http://news.gallup.com/poll/197444/americans-worries-crimes-similar-2015.aspx (accessed May 30, 2018).

governments provides powerful nodes between states that reduce the need for conventional forces (Clarke and Knake 2010). The dependence on the domain for everything from banking to military command and control orders allows precise cyber attacks to paralyze networks of choice with disastrous effects (Zheng 2015). This interconnected world gives cyber attacks "fantastically game-changing" capabilities that naturally and rationally create optimism and fear for the cyber domain.[66]

Rid's (2012) notion that cyber war is not something to be overly concerned with because cyber attacks are not physical, violent, or lethal does little to placate authors in this camp. For example, Stone (2013) argues that war is simply an act of force that compels the enemy to do your will. Liberal ideals of war seek to compel an enemy with the minimum loss of life possible (at least in theory). Thus, cyber attacks are the ultimate tool of liberal warfare. These liberal ideals of conflict seek to minimize loss of life by "employing advanced military technique[s] to strike rapidly and accurately at the material components of the enemy's means of resistance."[67] As a result, authors who believe optimism and fear of the cyber domain are overblown are merely unable to see that the cyber domain has changed the old vocabulary of war. To these authors, the optimism and fear for cyber weapons that this research project seeks to explain are natural reactions to a new style of warfare that scholars like Rid are unwilling or unable to see.

The authors who articulate this explanation, however, still fail to rectify their theories with empirical evidence. Thus far, we have seen little evidence that cyber attacks will (or can) compel an enemy at levels comparable to conventional forces. Terrorist techniques have shown the ability to coerce governments, as seen with the Taliban, Al-Qaeda, and ISIS (Kaldor 2012). Although these organizations may not meet their long-term strategic goals through their terrorist

[66] Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar – What Everyone Needs to Know.* New York, NY: Oxford University Press, 2014:133.
[67] Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies.* 2013:105.

acts, they have nonetheless achieved important goals from terrorism. I showed earlier, however, people fear terrorism at a lower rate than cyber attacks even though cyber attacks have shown little if any empirical evidence of their strategic ability to coerce governments, ruin economies, or kill people. Despite this, some scholars still assert that this new form of warfare is "being employed, and with genuinely damaging effects."[68]

These scholars offer up cyber weapons as a new and powerful form of warfare, yet they do little to justify why we should fear a weapon that has shown nearly no ability to alter the political calculus of state leaders. If the objective of all actions in war is to create a political reaction or change (Mahan 1890; Corbett 1911; Fuller 1926), then optimism and fear for a new weapon should be rooted in empirical evidence that the weapon can bring about such change (e.g., nuclear weapons). Thus far, there is no empirical evidence to support such a claim.

Theory

My theory hinges on two general propositions to explain why cyber fear and optimism exist without empirical support. First, fear arises from the inability to distinguish between the offense and the defense in the cyber domain. The lack of clarity between the two forms of war causes cyber operations to appear threatening even if the state undertaking the action has no offensive intentions. A cyber weapon designed to gather intelligence as part of a defensive operation could also be used offensively to paralyze a network. It is difficult for the targeted state to discern the purpose of a cyber weapon, and even if they could, the attacker could switch the purpose of the attack quickly due to the pervasive nature of the domain. The inability to discern intentions and objectives elevates fear levels among the public and elites.

In other domains, states can signal a defensive role for their arsenals of airplanes, soldiers, and ships with scripted defensive military exercises and preplanned training

[68] Arquilla, John. 2012:2.

deployments. It is a straightforward process to detect a change in this posture because states can monitor the deployment of an adversary's airplanes, ships, and soldiers with reliable accuracy. The ability to discern offensive operations from defensive ones creates clear signals and helps keep fear levels in check. Because this delineation does not exist in the cyber domain, cyber operations appear threatening and cause fear regardless of the intentions of the state undertaking the cyber operation.

Next, optimism arises from a pervasive belief in the efficacy of the offense over the defense. Cyber defense is not an exploitable concept as it is in other domains. State leaders cannot 'deploy' anything in cyberspace to defend against an impending cyber attack in the same manner they can deploy ships, soldiers, or airplanes to parry a conventional attack. Further, state leaders receive nearly no warning for imminent cyber attacks. Signals such as troop buildups or aircraft deployments generally precede attacks in the other conflict domains. The lack of these signals in the cyber domain means cyber defense must be all-encompassing and exist everywhere at all times. The requirement to sustain such a posture creates the perception that cyber defense is the status quo rather than a form of warfare that can be decisively employed as in other domains. Thus, people believe that a potent offense is the only exploitable concept in the cyber domain. Further, because persistent and complete cyber defenses are difficult-to-impossible, people have great optimism for offensive cyber attacks to succeed in future conflicts.

This theory relies upon two established concepts within IR literature. In a seminal piece on cooperation under a security dilemma, Jervis (1978/2003) explicates two variables that shape how states view threats. The first is whether state leaders can distinguish defensive weapons and policies from offensive ones. The second is whether leaders believe the offense or defense has

the advantage.[69] My theory relies on these two concepts to explain why we see elevated fear and optimism for cyber weapons without any demonstration events or empirical evidence to support such perceptions.

From these two concepts, I created two general cyber propositions that serve as the pillars in my theory. The first proposition is that people cannot easily distinguish between offensive and defensive cyber activity. An examination of the cyber domain shows that one of the primary reasons the line between the offense and defense is blurred is because creating strong cyber defenses requires, at least partially, on knowing the adversary's cyber capabilities. Offensive cyber operations are an efficacious means of gathering the intelligence required to make this assessment. Researchers have hinted at this problem in previous research, noting that the US promotes cyber security on the international stage, but consistency undermines those goals with offensive cyber operations designed for "intelligence purposes."[70] In short, strong cyber defenses rely on offensive cyber operations to provide the needed data.

Conceptually, this is important because when the offensive or defensive purpose of a weapon is unclear, it causes uncertainty, anxiety, and expectations of worse case scenarios. State leaders ease this worry by resorting to espionage to create firmer assessments of the intended purpose of a weapon. In today's environment, cyber espionage has become a cheap and highly effective method to gather the desired intelligence. Libicki (2009) notes, "states have little knowledge of exactly what [cyber] weapons are in the arsenal of their rivals."[71] Thus, governments need to probe other states' arsenals to bolster their cyber defenses. To achieve the desired cyber security goals, state leaders must mix the offense and defense. The driving factor

---

[69] Jervis, Robert and Robert Art. "*International Politics – Enduring Concepts and Contemporary Issues 6th ed."* Addison-Wesley Educational Publishers Inc, New York. 2003:180.

[70] National Research Council. *At the Nexus of Cybersecurity and Public Policy.* Policy Report, Washington DC: National Research Council, 2014: 102-105.

[71] Libicki, Martin. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009: 77.

for this progression is the central premise that strong cyber defenses rely, at least partially, on offensive cyber operations to glean the required intelligence.

Another reason the offense and defense are difficult to distinguish in the cyber domain is that cyber code created to gather intelligence for defensive purposes can quickly be turned into an offensive weapon. Cyber attacks that exploit backdoors for a state to gather cyber intelligence can also provide the conduit needed to undertake a potentially potent offensive attack. The former chief of the US Cyber Command, General Keith Alexander referred to this as "strategic instability" regarding interstate cyber activity.[72] Indeed, cyber scholars have noted the pliable and obfuscated nature of cyber operations has created only "rudimentary" principles of offense and defense that provide little foundation for decision-makers to rely upon when crafting policy.[73] The opacity of cyber offense and defense and the inability to understand the objectives of a given operation also explains research that shows many people bypass realistic probability assessments of receiving measurable harm from online attacks, and instead display elevated levels of fear despite data showing relatively low levels of actual damage.[74] The lack of a divide between offensive and defensive cyber operations is the centerpiece of this cycle that creates and sustains high levels of fear and causes unrealistic probability assessments.

Other weapons or forms of warfare with the potential to cause substantial economic losses and significant fatalities (e.g., terrorism) do not exhibit the same obscuration between the offense and defense. As a result, we do not see elevated levels of fear for terrorism despite the measurable economic damage and loss of life terrorists can cause. As noted earlier, fear of cyber attacks has always exceeded that of terrorism in Gallup polling. The imbalance between the low

[72] Alexander, Keith. Testimony transcripts from the US Senate Committee on Armed Services, Government Printing Office, Washington DC, April 15, 2010: 219.
[73] Kello, Lucas. "The Meaning of Cyber Revolution," *International Security*, 2013: 7.
[74] Mason, Stevenson, and Freedman, "Ever-present Threats from Information Technology: The Cyber-paranoia and Fear Scale," *Frontiers in Psychology*, 2014: 3.

levels of destruction caused by cyber attacks and the large percentage of people who fear cyber weapons is a result of the inability to distinguish between offensive and defense cyber operations. The gray nature of cyber weapons leads to anxiety, concern, and thoughts of worst-case scenarios because the weapon does not have a clearly-delineated purpose or role in international affairs.

The inability to distinguish between offensive and defensive cyber operations amplifies the security dilemma and increases fear because states cannot enact effective policies to counter the weapon.[75] Research shows fear exacerbates the security dilemma and fuel security spirals (Jervis 1976), can trigger destructive wars (Doyle 1997), and can alter military alliances (Horowitz, Post, and Stam 2017). My theory, however, does not explain what role fear plays in the cyber domain. Rather, my theory explicates the causal mechanism that creates such high levels of cyber fear in light of an unconvincing empirical record of cyber destruction and the questionable ability for the cyber weapons to alter state politics. The ability to distinguish between offensive and defensive weapons diminishes the security dilemma and reduces fear because states can enact policies that counter the specific weapon(s).[76] With the entanglement of the cyber domain into all aspects of state business and public life, the reliance on the domain for economic health, and the *inability* to distinguish adequately between offensive and defensive cyber operations, state leaders cannot enact credible policies to counter cyber threats effectively. Thus, despite an empirical record that shows the cyber domain brings an excellent upside and minimal losses, the public and political elites exhibit high levels of fear for cyber attacks.

The second theoretical concept elucidates why there is great optimism for cyber weapons to beneficially alter future conflict despite no demonstration event or record of accomplishment

[75] Jervis, Robert. 2003:191.
[76] Jervis, Robert. 2003:191.

to ground such perceptions. The optimistic view that cyber weapons can alter international politics is rooted in people's belief that the cyber offense has higher potential than cyber defense. I base my second general cyber proposition on the following premise: that people view cyber defense as the status quo and not as an exploitable concept that can offer measurable gains when compared to offensive operations. Simply put, the offense has the advantage in the cyber domain. Working in concert with this is the notion that cyber attacks can bypass traditional military domains. This belief creates perceptions that offensive operations are a panacea for traditional methods of conflict. Together, these two theoretical concepts fuel cyber optimism.

In the cyber domain, the offense/defense balance works differently than in other domains. Unlike the deployment of airplanes, ships, or soldiers to defend against hostile action when needed, the cyber domain requires a constant and pervasive defense. Because of the enmeshment of the cyber domain in all facets of economics and politics, states cannot relax this defense or 'put it in garrison' as with other domains. Therefore, people perceive cyber defense as necessary for standard functionality rather than an exploitable concept. Defense in the cyber domain is not a maneuver employed against an adversary at a given time and place as military leaders do with airplanes, boats, or soldiers. It is merely something that must exist everywhere and at all times.

The belief that the offense has the advantage in the cyber domain causes the optimism that people adopt regarding cyber weapons and future conflict. For example, NATO Supreme Allied Commander General Clark suggested in 1999 that cyber attacks, had he been given authority to use them (he was not), may have proven more effective in toppling Milosevic than the aerial bombing campaign undertaken by NATO forces. Such optimism remains prevalent today despite no significant cyber demonstration event, no deaths, and no widespread destruction

resulting from a cyber attack. This same process played out with the airplane in the early 20th century.

The ease at which the early airplane could overfly geographic boundaries created a near-immediate impression among all people that the airplane was an unstoppable offensive weapon. The lack of strategic vision that led many to buy into the aircraft's version of the cult of the offensive led to drastic funding increases for military aviation and separate and independent air forces for nations. Early proponents of airpower were so blinded by the ease at which aircraft seemed to be able to strike at the heart of enemy cities, that they believed "the mere *threat* of bombing a town by an air force will cause it to be evacuated, and all work in munitions and supply factories to be stopped."[77] As history tells us, however, societies and militaries proved far more resilient than expected when faced with aerial bombing campaigns.

Just as with cyber weapons today, defense against the airplane in the early 20th century was difficult, and this offense/defense imbalance seemed to alter the vulnerability of a state radically. Regarding early airpower, historian Peter Fritzsche notes, "invasions carried out along a single horizon were relatively easy to deter by means of troops, ships, and blockades. But aerial warfare opened up the entire sky and threatened to strike from innumerable directions."[78] The ease at which pilots were able to trespass over enemy territory created optimism for the weapon to strike at the time and place of a commander's choosing. Because of the firm belief in the offensive nature of the airplane, it did not matter that the empirical record showed little

[77] Mitchell, William "Billy." *Winged Defense: The Development and Possibilities of Modern Air Power – Economic and Military.* University of Alabama Press, Tuscaloosa AL. 1925/2009: 6.
[78] Fritzsche, Peter. *A nation of Flyers: German Aviation and the Popular Imagination.* Harvard University Press, Cambridge MA. 1992:204.

evidence that airpower could cause the widespread political upheaval or demoralization of the enemy that military and political leaders believed it could.[79]

Today, this same theoretical concept is at work within the cyber domain. The trust in cyber offense over cyber defense creates and sustains the optimism for these weapons to strike at an enemy with lethality and speed unmatched by other weapons. That data and history provide no grounds for such a belief are irrelevant in light of a cyber weapon's uncanny ability to bypass barriers to traditional military forces. The belief that cyber weapons can take out the "eyes, ears, brain, and nervous system" of a state and cause paralysis that leads to quick military victories is prevalent among military and political leaders.[80] For example, former US Senator Joe Lieberman (I-CT) stated in 2012 that offensive cyber weapons could "paralyze [a] nation with targeted cyber attacks on critical networks" and that such belief is "anything but hype."[81]

What causes the widespread belief that the offense is stronger than the defense in the cyber domain is a direct result of the domain's ability to bypass traditional mediums of kinetic power. Modern militaries have technology and doctrine to exploit offensive *and* defensive strategies for the land, sea, and air domain. However, the cyber domain offers a new tool to circumvent these barriers to power projection. The optimism leaders have in cyber weapons to alter future conflict is a result of the weapon's ability to circumvent other domains. People believe in the efficacy of offensive cyber operations not because there is reliable data that says this optimism is rational, but rather because cyber weapons seem to offer a technologically advanced, bloodless, and quick method to overcome traditional forces.

---

[79] Overy, Richard.. "The Air War in Europe, 1939-1945. in *A History of Air Warfare*. by John Olsen, 27-52, Potomac Books, Dulles VA. 2010:24.
[80] Pollpeter, Kevin. "Chinese Writings on Cyberwarfare and Coercion." In *China and Cybersecurity*, by Jon Lindsay, Tai Cheung and Derek Reveron, 138 - 162. New York: Oxford University Press, 2015
[81] Quigley, Kevin, Calvin Burns, and Kristen Stallard. 2015: 113.

The primary testing method for my theory is a survey experiment of 1,000 US residents. A valid concern about this approach is the possibility that elites and cyber experts who craft international cyber policy may have insider information that nullifies some or all of my theoretical tenets. To test whether this is the case, I also administer an identical survey experiment to a small group of cyber experts to identify if their responses are statistically different from the larger population sample. I theorize that I will find no statistical difference in their responses for two reasons. First, an analysis of speeches and policy positions from decision-makers shows a strong inclination towards the type of positions I outline in my theory. If having access to greater information on cyber operations nullifies or dampens my causal mechanisms, we should see less expert rhetoric and hyperbole regarding cyber operations and the harm they do or can cause. As shown throughout this chapter, this is not the case.

Second, as someone who has had previous access to insider information on cyber operations, it is my experience that the increase in information only exacerbates the difficulty in discerning clearly what is happening and what the ramifications are of different operations. I believe this is what has led those with the most amount of insider information, like General Alexander, to note the significant instability the domain causes for decision-makers. While I hypothesize that I will find no difference between the expert sample and the general population sample, I believe I may find stronger results for my theory among government cyber experts because of the problems decision-makers face with vast amounts of indiscernible cyber information.

Plan for the Dissertation

The goals for the next three empirical chapters are: (1) determine if there is support for my proposition that the early air domain and the modern cyber domain created similar

perceptions in the early years of each domains' development – this will validate the generalizability of the theory, (2) examine data from two unique survey experiments to assess support for the causal mechanisms I identified in my theory, and (3) assess how these causal mechanisms influenced cyber policy development in the US from the birth of the modern cyber domain in the 1980s until the 2014.

In Chapter Two, I offer a comparative analysis of the development of the air domain in the early 20th century and the development of the modern cyber domain. Elites and the public exhibited similar perceptions in the early stages of each domain, and I will evaluate whether the same causal mechanisms were at work in both cases. While some researchers have obliquely noted that the modern cyber domain and the early air domain showed similar properties, none have offered an empirical evaluation of the similarities, nor have they offered any theoretical principles to explain why these similarities exist. The comparative analysis I offer in Chapter Two will broaden the generalizability of my theory beyond the cyber domain by aligning general causal mechanisms between the two domains. Additionally, I analyze how the tenets of my theory resulted in specific outcomes for both the early air domain and the modern cyber domain.

I compare perception development in the air domain against the modern cyber domain for three reasons. First, early airplanes allowed people to utilize the domain in a very similar manner to cyber. It provided a method of communication, allowed new economic growth and opened up new military opportunities. Much like the cyber domain, the early air domain provided benefits to all (e.g., air travel, mail service), yet could only be mastered by those with specialized training and knowledge (e.g., pilots). Second, there was a fear and optimism for early airpower that is mirrored in the modern cyber domain. This occurred in both domains before any demonstration event or data to justify the perceptions. Third, scholars have noted the

similarities between the development of both domains (see Nye 2017; Arquilla 2015; Libicki 2009) but have not undertaken any scientific projects to determine why we see such similarities. Thus, a historical comparison between the two domains provides fertile ground for new scientific findings.

During the comparative analysis, I rely on public statements from elites, congressional documents, scholarly work, and other sources to highlight the causal mechanisms I identify in my theory and show how they worked for each domain and what the outcome was/is. Juxtaposing the growth of the air and cyber domains help alleviate concerns that developing sound cyber theories are too difficult because of the rapid innovation in the cyber domain, disagreement about the domain's influence on state affairs, and the complex and technical nature of cyber operations. Illustrating the comparable nature of the two domains overcomes this and other concerns by showing that many similar properties exist between the two domains.

In Chapter Three, I analyze the results of a survey experiment on 1,000 US respondents. I examine the data to determine if there is support for my propositions by testing six hypotheses that represent various facets of the theory. Positive results from the experiment will allow me to offer the first cyber theory supported by data collected from a survey experiment. This approach diverges from traditional cyber research that generally utilizes existing aggregate-level cyber data without an empirically founded theory to explain the findings (see Lewis 2013; McGraw 2013; Rid and McBurney 2012; and Singer and Friedman 2014). I also conduct an identical survey experiment on a sample of 64 cyber experts to determine if their responses differ from the general population. These experts have experience in the cyber field either from academic research or from various government positions within the DOD.

In Chapter Four, I conduct a process-tracing study of the development of US cyber policy from 1986 to 2014. This analysis tests how my causal mechanisms functioned and how they impacted policy development and implementation. I will draw upon cyber-related budgets, congressional hearings and testimony, and organizational changes within the US government. My objective is to evaluate the degree to which my causal mechanisms shaped US cyber policy. For instance, were there cyber attacks that caused elevated levels of fear among the public and elites that resulted in policy changes? What actual damage did the attack(s) cause? Is there evidence that elites undertook major policy changes in response to cyber attacks that caused no damage or loss? Do their statements and the resulting policy changes support my theoretical propositions? The process-tracing structure will help identify how these perceptions shaped the way elites prioritized government resources at key junctions during the development of the cyber domain. For instance, the agent.btz cyber attack of 2008 helped spur the development of US Cyber Command. I will examine elite decisions and statements before the creation of the new military command to identify if and how my theoretical propositions influenced resource allocation and policy implementation during this critical juncture in US cyber policy.

Lastly, I conclude in Chapter Five by presenting a summary of the results, modifications to the theory, and areas for future research. The structure of this project allows me firm footing to make these recommendations because of the use of a survey experiment to collect cyber data while offering a comparative analysis of the cyber and air domains. The survey experiment offers a real-time assessment of cyber perceptions, while the comparison between the air and cyber domains provides a historical grounding for my recommendations. I also elaborate on how my research reshapes cyber literature and our lexicon of cyber conflict. Results in line with my

theory would portend the need for researchers to refocus on long-term global political trends that we might expect given the similarities between the air and cyber domain.

CHAPTER 2

A COMPARATIVE ANALYSIS OF THE EARLY AIR AND MODERN CYBER DOMAINS

Introduction

At present, modern theories about interstate cyber activity and the influence of the domain on global politics generally fail to capture broader concepts at work within the domain. These theories give some explanations for why a state might undertake cyber activity against another state, or how one state may react to a given volley of cyber attacks, but they do not offer any explanation for the underlying perceptions of cyber attacks held by the public and elites that drive much cyber foreign policy. This lack of theoretical foundations decreases the generalizability of the theories because they are not grounded in concepts that allow an application of the theory across time and space.

For example, Valeriano and Manass's (2015) theory about cyber activity suffers from a lack of generalizability because their cyber attack data comes only from dyadic rivals rather than all nations. While this was a purposeful choice by the authors, it is typical of trends within the cyber research field to focus on subsets of cyber activity without first establishing generalizeable concepts for the domain. Because of this, the cyber research field as a whole has yet to offer empirically supported theories grounded in proven international relations concepts. The result is cyber research that does not explain how characteristics of the cyber domain influence outcomes. Instead, most of the cyber theories generally seek to clarify how specific interactions (e.g., cyber attacks between rivals) influence decision-makers and shape outcomes, rather than examining how preexisting beliefs and perceptions impact decision making.

My theory differs in that it utilizes innate characteristics of the cyber domain to explain observed outcomes, rather than using a subset of interactions between actors. Because of this, I can generalize my theory to other domains that exhibited the same characteristics and test whether my theory and hypotheses generalize beyond the cyber domain. The purpose of this chapter is to determine if there is qualitative evidence that the domain characteristics I identify have a substantial influence on perceptions and whether these extend to other domains with traits similar to those of the current cyber domain. The goal of this chapter is to determine if the concepts I theorize are at work in the cyber domain also influenced perceptions about the new air domain a century ago. If so, the research will shed light on generalizeable concepts that drive domestic and international policy in the early stages of a new domain.

The previous chapter argued that an overriding belief in the offensive capabilities a new domain offers creates feelings of optimism. This optimism leads elites to believe the new domain will radically alter warfare and pay high dividends to the state that best harnesses the new technology. The creation of such optimism occurs because the apparent efficiency of the offensive form of war in the new domain appears so groundbreaking that it causes elites to believe it to be a panacea to convention conflict. The theory also asserts that fear is created when defensive and offensive operations and intentions are difficult for other states to distinguish. The result is elevated fear because political and military leaders cannot craft effective policies and military postures to counter the threat.

Indeed, this creates situations where leaders may not even agree whether a threat exists or not. In this chapter, I apply these theoretical tenets in a direct comparison between the early air domain and the modern cyber domain to determine if these causal mechanisms operated similarly during the development period of each domain. Such evidence would bolster the

generalizability of my cyber theory by showing that the foundations of the theory are grounded in concepts that apply across time and between domains.

To meet these objectives, I conduct an empirical comparison between the early air domain (1903 to 1939) and the modern cyber domain (1986 to present). These two domains and periods differ in such substantial ways that logically we would not expect the theory to work similarly for the two domains. The most apparent difference is nearly 100 years between the births of each domain. During the birth of the air domain, the early 1900s saw growing industrial economies, a disparate global political landscape fraught with signs of an impending world war, limited and basic communications systems between citizens, elites, and states, and sparse time-delayed global news coverage.

This stands in stark contrast to the period of growth for the modern cyber domain, which showcased interconnected advanced economies, a united global political landscape (e.g., UN, IMF, WTO) that worked proactively to avoid massive wars, direct and immediate communications between citizens, elites, and states, and real-time global news coverage available to nearly all citizens. Despite these immense differences, I posit that the causal mechanisms worked in nearly identical forms for both domains because I base the theory on human perception development of unchanging offensive and defensive principles of war. I argue that these principles apply just as much in the modern cyber domain as they did in the early air domain 100 years ago.

I have chosen the periods under investigation for each domain for several reasons. The air domain became viable for military use when the Wright brothers demonstrated the ability to sustain powered flight with their test flights at Kitty Hawk in 1903. Aircraft before this consisted either of balloons or dirigibles used for research or basic military tasks like

reconnaissance. While it took several years after Kitty Hawk to construct powered aircraft that could fly for significant periods, public and private discussions on the impact of powered aircraft on foreign policy and future conflict began in earnest around 1903.

During the years from 1903 to 1919, I theorize that the fear that existed about the air domain was due to the uncertainty over what type of roll (offense or defense) aircraft would play in future conflicts. The embryonic state of aviation in this period left far more questions than answers regarding the airplane's role in warfare. The lack of distinction between what precisely this new weapon would provide for nations that opted to pursue the technology meant that no government could craft effective policies to contain or manage an adversary who was exploiting the new domain. The worst-case scenario political leaders had to consider was that aircraft possessed radical offensive firepower that would alter warfare, make land and naval forces obsolete, and leave cities defenseless against aerial attacks. The best-case scenario was that aircraft would add only limited communication and reconnaissance capabilities that would help land and naval forces defend themselves and their nations. The vast lacuna between the competing ideas caused fear and anxiety because political and military leaders could scarcely formulate policies or create military postures that provided adequate defenses against the new weapon.

During the second period from 1920 to 1939, the same causal mechanism existed that caused fear, but the pathway differed. Fear did not exist because elites and the public could not determine what role aircraft would play in future conflicts. During this time, the aircraft demonstrated the ability to execute both offensive and defensive missions with general effectiveness. Now, the fear that existed did so because people could not accurately assess the intentions of another state that chose to build up its air force because aircraft could execute either

highly offensive or highly defensive missions. As my theory explicates, this causes fear and anxiety because the purpose of a state's growing air force could not be delineated. Without a distinction between the offense and the defense, no state could ascertain another state's intentions and create effective foreign policies.

I chose 1939 as the end date for the air domain analysis because this effectively marks the end of the early development period of the air domain. By the beginning of WW2, most nations had standing air forces, had a stable set of preferences for how and why they might employ their aircraft, and generally had a grasp on what the airplane could or could not do. I do not claim that the development of the air domain stopped at this point, or that the set of preferences and beliefs developed up to this point regarding the ability of airpower to alter wars were correct. Indeed, Allied trust in the efficacy of strategic air bombardment proved misplaced during the early years of WW2, with airpower falling short of many expectations. What WW2 provided for governments, however, is something that had been vastly limited in the period from 1903 to 1939: immense amounts of raw, real-world data on the effectiveness of aircraft in combat. Because my theory seeks to describe and explain forces at work on perceptions *before* empirical data is available to support these perceptions, I end my research on the air domain at 1939.

My research on the cyber domain starts in 1986 and ends in 2014. There is no clear beginning to the cyber age, as the progression from analog electronics to a digitally connected world happened gradually. However, starting around 1986, there is a distinct movement within the US government and corporations to upgrade their disconnected analog systems to interconnected digital systems. While the internet and digital communication devices were at work before 1986, the computers were generally segmented and offered limited

interconnectivity. As of 1986, 40 percent of the world's general-purpose computer power resided in pocket calculators, which, when combined, accounted for more capability than all personal computers worldwide.[82] The year 1986, however, marks the time when the sales of digital and interconnected computers began to grow exponentially. From the late 1970s until 1986, annual sales rates for personal computers went from approximately zero to roughly 10 million units worldwide. By 1990, this figure grew to 20 million, and by 2000 it was around 140 million.[83] Cyber researcher Jason Healey also identifies 1986 as the year of the first veritable cyber attack, with German-backed hackers transferring sensitive data on President Reagan's Strategic Defense Initiative from the Lawrence Berkeley National Laboratory to their KGB handlers.[84] My research ends with an analysis of the Stuxnet attack, which had effects from 2010 to roughly 2014.

Questions for the Comparative Analysis

My analysis of the two domains and periods identified requires a controlled case study approach to present the most accurate qualitative research. This approach means asking the same questions for each case study to determine if the results are similar enough to lend support to my theory. My theory seeks to explain the fear and optimism we see for both domains, and as such, I start each case study with the goal of identifying the fear that elites and the public held for each domain. While I cannot quantitatively determine the level of fear, I seek to understand how common fear was among the public and elites through public statements, government reports, and transcripts of government hearings on both air and cyber security. My next objective is to determine if historical records give any indication of why people felt this fear. My theory says

[82] Mayer-Schonberger, Viktor and Kenneth Cukier. *Big Data*. New York, NY: Houghton Mifflin Harcourt Publishing Company. 2014: 9.
[83] Reimer, Jeremy. *Personal Computer Market Share 1975-2004*. http://www.retrocomputing.net/info/siti/total_share.html (accessed October 5, 2018).
[84] Healey, Jason. 2013:7.

this fear rests in the obfuscation between the offense and the defense, and thus I look for evidence that this played an outsized roll in the creation and sustainment of this fear.

Next, I examine the optimism people held for each domain to alter future conflicts beneficially. I first look to determine the prevalence of this optimism, and then I consider what provided the foundation for such a perception before empirical evidence was available to justify it. My theory presupposes this is due to the overwhelming belief in the efficacy of the offense over the defense for the new domain. As with my research into the perceptions of fear, I seek to understand why this optimism existed and what, if any, role my causal mechanism played.

Early Air Domain – 1903 to 1915

The year 1903 marks the beginning of the powered age of air flight and the growth of fear and optimism about the machine's capability to inflict immense harm on an adversary. Fear of weaponized air machines certainly existed before the Wright brothers' flight in 1903. Parisians reacted to balloon flights over France in the 18th century by predicting that weaponized balloons would leave "our cities on fire, our harvests ravaged, our fortresses destroyed" and their wives and daughters harmed by "lovers and thieves descending our chimneys."[85] This fear was widespread among politicians, the public, and scholars. In 1888, Polish scholar Ivan Bliokh called flying machines, "a danger before which the world cannot remain indifferent."[86] Yet balloons and dirigibles lacked speed and maneuverability and were often at the mercy of capricious winds, limiting their usefulness in combat. Powered flight overcame these limitations and brought capabilities that opened up an entirely new realm of possibilities. The airplane's ability to overfly geographic obstacles and common land defenses, along with the unclear

[85] Hunn, James. "Popular Science in Paris in the 1780s: The Example of Ballooning." Unpublished Paper.
[86] Kennett, Lee. 1991: 1.

offensive/defensive capabilities they possessed, created and sustained a new level of optimism and fear that would propagate worldwide and continue unabated for decades to come.

The initial reaction from the US government to the Wright brothers' first powered flight was hesitation. Despite the fear brewing among elites and the public over the potential use of aircraft in future conflicts, the US government put little effort into exploiting the new domain for offensive purposes and even less for defensive purposes after the events at Kitty Hawk. As of 1907, the only US military office dedicated to aviation was an Army Signal Corps unit that consisted of just one officer and two enlisted soldiers.[87] Even this office, however, sought to utilize the aircraft only for surveillance and communication purposes. The seemingly little interest from US government officials after Kitty Hawk led the Wright brothers to extend their search for a government willing to fund their requests for further aircraft development. Between 1903 and 1908, the Wright brothers negotiated with the British, French, and German militaries in hopes of securing a contract for aircraft purchases.[88] None of the negotiations resulted in contracts, however, and the Wright brothers did not fly again until 1908.

During this same period, governments around the world struggled to understand what the airplane's role would be in wartime. Governments were generally unwilling to invest the money required to develop the technology needed to build aircraft that met the high expectations many held about its role in conflict. Early investing by the US and many European governments sought to develop the aircraft for defensive purposes like reconnaissance and signaling. Despite the hesitation of governments to fund research and development for offensive purposes, political leaders began engaging in discussions to delineate the aircraft's role in offensive combat under international law.

[87] Biddle, Wayne. *Barons of the Sky*. Baltimore, MD: Johns Hopkins University Press. 2001:41.
[88] Morrow, John. *The Great War in the Air*. Washington DC: Smithsonian Institution Press. 1993:5.

A peace conference at The Hague in 1907 resulted in a draft agreement that restricted aircraft from bombing undefended towns and villages.[89] While this signaled the offensive potential that some elites saw in the airplane, few governments were willing to commit the money required to develop aircraft into a weapon that would meet these expectations. Here we find the first evidence of the obscuration between the offense and the defense for the developing air domain: governments were mainly investing in aircraft for defensive roles like signaling and reconnaissance, while at the same time, elites were discussing the wild possibilities the aircraft brought on the offensive front. The ambiguous offensive/defensive characteristics of the new air domain caused fear and anxiety among the public and elites in the following years. This ambiguity continued until approximately 1919 as governments struggled to understand the offensive and defensive capabilities of aircraft.

As the aviation industry grew in the looming shadow of WW1, early airpower theorists often cast the aircraft's role in strictly defensive terms. One of the most well known of the early airpower advocates was General William "Billy" Mitchell. Mitchell became a rising star in the US Army Signal Corps in the early 1910s and quickly saw the potential the airplane offered to conventional military forces. Mitchell once stated that the advent of airpower "completely changed all former systems of national defense" and thus required a separate and independent military branch to harness the aircraft's true potential.[90]

Even as Mitchell made very public and vocal pitches for an independent air force for national defense (his widely published 1921 book was titled *Winged Defense)*, Mitchell also pushed to showcase the offensive ability of the aircraft to alter future wars. His efforts culminated in his staged bombing of the captured German warship the *Ostfriesland* in 1921.

[89] Morrow, John. 1993:9
[90] Mitchell, William "Billy" *Winged Defense*. Tuscaloosa AL: The University of Alabama Press. 1925/2009: xiv.

Mitchell and his fellow pilots successfully sunk the ship and made a spirited attempt to utilize the event to showcase the offensive ability of the aircraft, despite Mitchell's very public opinion that the aircraft was best suited for defensive purposes.

In short, even one of the most well-known airpower advocates from the beginning of the air domain could not articulate a clearly defined offensive or defensive role for the aircraft because there *was* no clearly defined role. The embryonic state of the new air domain made an offensive and defensive delineation difficult. This vagueness meant governments struggled to craft effective policies against the new weapons, which in turn caused fear. As Jervis (1979/2003) postulates, the inability to distinguish between offensive and defensive weapons increases fear because states cannot enact policies that counter the specific weapon(s).[91] The grey nature of the aircraft's role in conflict caused fear that extended beyond military and political leaders, however.

Noted author H. G. Wells wrote in his 1908 fiction *The War in the Air* that a relatively light air attack on New York City forced a quick surrender by confused and scared politicians.[92] The air attacks, Wells wrote, would not cause national surrender as some believed but would stoke a fiery nationalism that would plunge the nation into total war. This type of hyperbole took place at the same time across the Atlantic. Frenchman Louis Bleriot's flight across the English Channel in 1909 prompted the *Daily Mail* to publish an article the day after the event that said, "British insularity has vanished. We would not be understood to say that in a few weeks or months hordes of aeroplanes will follow where M. Bleriot has led, but his example has shown the way… The British people have hitherto dwelt securely in their islands… But locomotion is now being transferred to an element where Dreadnoughts are useless and sea powers no shield

[91] Jervis, Robert and Robert Art. "*International Politics – Enduring Concepts and Contemporary Issues 6th ed.*" Addison-Wesley Educational Publishers Inc, New York. 2003:191.
[92] Wells, H. G. *The War in the Air.* New York, NY: George Bell and Sons. 1908.

against attack."[93] Even well-respected scientists made predictions about the offensive effectiveness of airpower, with Thomas Edison once quipping that the airplane could destroy a large city in five minutes despite having never proven its ability to inflict even moderate damage to small towns at the time of his statement.[94]

The rudimentary nature of these early ideas about airpower's role in warfare and the inability for anyone to make sense of the offensive or defensive purpose of the weapons created strong perceptions of fear for the new air domain. While wildly creative ideas about the aircraft's ability to plunge large cities into blazing infernos ran rampant among the public and political elites, others felt the aircraft only held the potential for defensive missions like coastal reconnaissance. In 1913, the assistant US secretary of war stated that, while the role of the aircraft may change in the future, it currently only provided "merely an added means of communication, observation, and reconnaissance."[95] Indeed, even the French military, long an advocate of developing airpower, entered WW2 in 1914 with only 141 aircraft, all of which were dedicated exclusively to defensive missions.[96]

The divided opinions on the new air domain's role in future conflict caused fear and angst among many and left more questions than answers. Historian Michael Sherry sums up the plight this presented to elites in the early years of the air domain by noting that:

> Those who thought about the future of air war… had few alternatives from which to choose. They were told that terror from the sky would eliminate the burden of carnage on the ground and costly armadas at sea by shocking armies and nations into quick surrender and perhaps even into permanent peace. Or they could take comfort in the assurance that the airplane

[93] Gollin, Alfred. *The Impact of Air Power on the British People and Their Government*. Macmillan, London. 1989: 72.
[94] Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing.* Princeton University Press, New Jersey. 2002: 148.
[95] McClendon, R. Earl. *The Question of Autonomy for the U.S. Air Arm, 1907-45.* Maxwell AFB, AL: Air University Press. 1950:33.
[96] Morrow, John. "The First World War, 1914 – 1919." In *A History of Air Warfare,* by John Olsen. Dulles, VA: Potomac Books, 2010:5.

would scarcely change warfare at all, serving only to improve observation and communication (as balloons were already doing) or to add a bit of firepower to the battlefield.[97]

The lack of clarity over what the airplane could or could not do began to change when WW1 offered governments initial empirical evidence that helped them form a clearer picture of the aircraft's potential. During the first year of WW1, aircraft contributed little to the war effort beyond reconnaissance and limited (and mostly ineffective) aerial bombing. The German military utilized the aircraft as a "supplementary means of information relied upon principally for confirmation" of operational reconnaissance.[98] The British employed their aircraft in much the same manner, with coastal defense units patrolling the English Channel for invading armadas. In 1915, however, newer technology and doctrine propelled the aircraft into a subtlety more offensive role.

Early Air Domain – 1915 to 1925

Larger aircraft with more powerful engines allowed commanders more opportunities to test the aircraft's ability to bomb enemy targets and shoot down other aircraft. In 1915, the French Voisin biplane began carrying 155mm artillery shells that it could drop on targets, while the new German Fokker *Eindecker* monoplane was edging into an offensive role as an air-to-air fighter plane. British naval aircraft, once relegated to coastal defense, began undertaking bombing missions against German targets in Belgium. The results of the aircraft's first real foray into offensive missions during 1915, however, produced few empirics to support the perceptions of fear and optimism. A report of French and British aerial bombing efforts in 1915 showed that of 141 attempts to bomb enemy railway stations, only three attacks (2.1 percent)

[97] Sherry, Michael. *The Rise of American Air Power – The Creation of Armageddon.* New Haven, CT: Yale University Press. 1987:8.
[98] Morrow, John. 2010:7.

produced hits close enough to be called useful.[99] Even the effective attacks, however, were merely symbolic because the munitions dropped at the time had little destructive potential. The limited success of offensive bombing attacks at this time was not the aircraft's only shortcoming, however.

Despite the initial push by governments to employ the aircraft into a defensive role leading up to WW1, there was much to be desired with the aircraft's defensive performance. British attempts to defend its coastline from German Zeppelin attacks in the early months of WW1 failed to stop many of the slow and vulnerable airships. By the end of WW1, German Zeppelins had dropped over 500,000 pounds of munitions on the British mainland, killed or wounded nearly 2,000 people, and caused much concern over British defenses.[100] In reaction to the inability of airplanes to stop the slow-moving Zeppelins, Sir Alfred Rawlinson of the Royal Naval Volunteer Reserve stated there was "a feeling of dismay [over the attacks]… following by a deep and universal anger that such attacks should be made upon our defenceless women and children."[101] In short, the airplane had little offensive or defensive success up to this point.

As WW1 progressed, advances in airdropped munitions, precision bombing sights, air-to-air machine guns, navigation, and the airplanes themselves made the aircraft a much more lethal machine for both offensive and defensive missions. According to historical analysis, however, "strategic aviation in fact played little role in the 1914-1918 conflict" and produced "limited and inconclusive" evidence of the airplane's ability to alter conventional conflict.[102] American reports on the airplane's effectiveness of specific air battles support this bleak assessment. Reports detailing the damage caused by aerial attacks against a critical rail junction in

[99] Kennett, Lee. 1991: 51.
[100] Biddle, Tami. *Rhetoric and Reality in Air Warfare.* Princeton, NJ: Princeton University Press. 2002: 22.
[101] Rawlinson, Alfred. *The Defence of London.* London: Melrose. 1924:4-5.
[102] Morrow, John. "The First World War, 1914-1918, in *A History of Air Warfare*. by John Olsen, 3-26, Potomac Books, Dulles VA. 2010:24-25.

Ludwigshafen showed that the majority of damage inflicted on the depot was not from the concerted effort to damage the facility with aircraft bombing runs, but rather from "falling shells and debris from German anti-aircraft guns" in the area.[103] Despite this, airpower advocates such as Mitchell claimed: "Aeronautics ended up on the Western Front as one of the decisive factors in all operations."[104]

US Army Major General Paul Malone also noted the ineffectiveness of the airplane during WW1 in his congressional testimony in 1934 about the future of the aircraft in a conventional conflict. General Malone stated that during the 1918 Chateau Thierry operation, his ground forces were attacked relentlessly by "about 5,000" German aircraft, but after many days his only losses to such attacks were three horses.[105] Historical records show that this lack of personal belief among those with military experience regarding the usefulness of the airplane in combat was rampant. Robert Grattan notes that the British Royal Flying Corps, which many considered much more organized and advanced than US military aviation in WW1, only attracted members because of "the excitement and novelty of flying rather than a deep belief in its military applications."[106]

Further, those that were attracted to the air corps, such as US Army Lt General Barney Giles, recall that his US Army flight training in 1917 was so poorly organized that after months and months in the Army pilot training program he had only logged four hours of flight time due to a shortage of airplanes and instructors.[107]

---

[103] Biddle, Tami. 2002: 64.
[104] Mitchell, William Brig. Gen. *Tactical Application of Military Aeronautics.* Undated memo written by Mitchell after WW1: 1. Air Force Archives Call 248.211-65K.
[105] US War Department. *Testimony before The Special Committee on Army Air Corps.* Washington DC: Columbian Building. May 17, 1934: 2478. US Air Force Archives Call 167.66-1.
[106] Grattan, Robert. *The Origins of Air War – The Development of Military Air Strategy in World War 1.* New York, NY: Tauris Academic Studies. 2009: 55.
[107] USAF Oral History Program. *Historical Documentation – Lt General Barney McKinney Giles.* Washington DC: Department of the Air Force. October 1966: 7. Air Force Archives Call K239.0512-779.

The fear of the early air domain that existed up to the close of WW1 remained prevalent because there was no clear delineation between the offense and the defense for the aircraft. While there was wild speculation about the airplane's capabilities in both forms of combat, the actual performance of the aircraft to this point left many wondering what its real role in future combat would be. Just as Jervis asserts with a new weapon, this caused anxiety among elites and the public because there was no practical way to counter a weapon that seemed to be on the cusp of changing warfare forever, yet produced little clarity for its real potential in either mission.

Post WW1, the role of aircraft and its true capability began to emerge. The fear that existed up to the conclusion of WW1 existed because there was no explicit offensive or defensive role for the airplane. This uncertainty began to change after WW1 because continued progress in technology, military doctrine, and peacetime testing produced aircraft that were capable in both offensive and defensive missions. The English Channel could no longer protect the British because a mainland European air force could overfly it and deliver powerful offensive blows. Even the vast oceans protecting America shrunk immensely as aircraft range and speed transoceanic flights.

Along with this, the aerial munitions of earlier years that had left much to be desired during WW1 battles, transformed into much more precise and lethal weapons in the interwar years. The new faster, higher-flying aircraft also performed well at defensive missions like coastal defense and reconnaissance. In short, the fear that existed in the interwar years did so because aircraft became so well suited for both tasks that it was nearly impossible for political leaders to distinguish what the intended purpose of another state's air force was.

The transition from aircraft that had no apparent purpose to airplanes that were capable in both offensive and defensive missions did not happen immediately. By the end of WW1, the US

government had spent approximately $100 million for a "winged cavalry of American warplanes that never materialized."[108] In the years following WW1, the US government did little to rectify the lack of aircraft development for either commercial or military use. A 1923 US Army report showed that the aviation arm of the service was in “alarming” condition, was practically demobilized, and that 80 percent of its nearly 2,000 aircraft were obsolete.[109] A committee of officers appointed by Secretary of War to investigate US military aviation in 1923 also determined that the air service was in “very unfortunate and critical” condition.[110] An internal US Army proposal published in 1922 strengthened these concerns, as it recommended the Army maintain its current 120 attack planes over the next ten years and suggested only a modest increase in bombers, from 146 to 204, by 1932.[111]

General “Billy” Mitchell saw the flagging state of US aviation, both in WW1 and shortly after, and began a very public campaign to garner support for commercial and military aviation. Mitchell was an extroverted and hard-charging officer with a reputation for speaking his mind. Mitchell served as the ranking officer of the Air Service on the European front during WW1, during which time he became even more convinced of the military efficacy of a dedicated aviation branch than he was before the war. During the Meuse-Argonne offensive in September 1918, Mitchell commanded a force of over 1,400 aircraft against German positions and won multiple awards for his service.[112]

In 1921, Mitchell made a public effort to convince government officials and the public of the offensive capabilities of aircraft by attempting to sink a submarine and several naval ships

[108] Biddle, Wayne. 1991/2001: 113.
[109] US Army. *Report of the Select Committee of Inquiry into Operations of the United States Air Services*, 68th Cong., 1st sess. Congressional Inquiry, Washington DC: GPO. 1925:4-5.
[110] US War Department. *Report of a Committee of Officers.* Washington DC: March 17, 1923: 5. Air Force Historical Archives File 145.93-102A.
[111] US Army Air Service Strength Report, June 23, 1922: 32. Air Force Historical Archives File 145.93-102.
[112] Biddle, Wayne. 1991/2001: 121.

with a fleet of airplanes. The first of Mitchell's attacks came in June of 1921 as he and a group of pilots bombed the captured German submarine U-117 just off the eastern US coast. Three flying boat aircraft made two passes over the anchored submarine and dropped 180-pound bombs on the vessel. After the second pass, the submarine sank when it sustained a direct hit, which split the hull in two.[113] Mitchell stated that the test caused discussions that night to wax "stronger than ever" and that those who observed the test from the Naval Transport Henderson "spent the night in terrific arguments" about the true offensive capability of aircraft against naval vessels.[114]

The next two tests were carried out shortly after this against the captured German torpedo destroyer G-102 and the cruiser Frankfurt. The attacks against G-102 went smoothly, with Mitchell noting that the attack "was beautiful to watch; the accuracy of the bombing was remarkable, practically every bomb went where it was directed" and that "everyone was surprised at the great accuracy" of the attacks.[115] After several bombing runs, G-102 was split in two and sank. The next test against the Frankfurt was not designed to sink the ship. Instead, Mitchell and his crew were to drop several variants of sand-filled inert bombs weighing up to 600 pounds. The intent was to impact the ship with several direct hits and then let military engineers inspect the damage as part of an effort to understand the impact of direct hits. Much to the amusement of Mitchell, and the dismay of naval officials, the last sand-filled 600-pound bomb dropped on the Frankfurt caused enough damage to sink the ship in short order.[116]

The last test Mitchell conducted in 1921 was the most important. Mitchell had secured permission to bomb the captured German battleship Ostfriesland. Mitchell noted that "This was

[113] Mitchell, William "Billy." 1925/2009: 57.
[114] Mitchell, William "Billy." 1925/2009: 58.
[115] Mitchell, William "Billy." 1925/2009: 61.
[116] Mitchell, William "Billy." 1925/2009 66.

our real test. If we could not sink this great ship the efforts against the other small vessels would be minimized and the development of air power against shipping might be arrested, at least for the time being."[117] The first set of attacks against the Ostfriesland inflicted moderate damage, which caused the ship to list. The following day, Mitchell and his crew found the ship still listing with the stern partially sunken. After receiving clearance to attack the ship, Mitchell's crews released four 2,000 pound bombs that struck in rapid succession. Reports indicate the attacks caused the Ostfriesland to fall on her side within a minute, go upside down within three minutes, and be nearly completely submerged within four minutes.[118]

The results of these tests seemed to provide the empirics needed to justify the fear and optimism that had existed up to this point without such evidence. Mitchell noted as much, saying that the sinking "ended the first great air and battleship test that the world has ever seen" and that it "conclusively proved the ability of the aircraft to destroy ships of all classes on the surface of the water."[119] At a public address in 1924, the Chief of the US Army Air Service General Patrick echoed these remarks, stating that the tests of 1921 "proved conclusively that bombs delivered from aircraft could put out of action or sink any naval craft which is up to this time has been designed or built."[120] The tests ensconced the offensive ability of the airplane that had not existed up to this point, yet they proved nothing of the combat ability of the plane.

The tests were carried out against moored and undefended vessels with scripted and controlled rules for the attacks. Combat would afford no such luxuries, and thus the tests offered nothing more than the knowledge that sinking large ships with aircraft was technically possible in peacetime, rather than realistically feasible in combat. While the range, speed, and lethality of

[117] Mitchell, William "Billy." 1925/2009: 66-67.
[118] Mitchell, William "Billy." 1925/2009: 72.
[119] Mitchell, William "Billy." 1925/2009: 73.
[120] Emme, Eugene. *The Impact of Air Power – National Security and World Politics.* Princeton, NJ: D. Van Nostrand Company, Inc. 1959: 47.

aircraft increased with each new model produced, there was still no empirical evidence that justified the perceptions of fear and optimism that existed. There was no data that supported feelings of vulnerability from nations that once felt relatively safe from attack due to geography (e.g., America, Britain), nor was there data to support the idea that a large air force could quickly overwhelm an adversary and force a quick surrender.

Early Air Domain – 1925 to 1939

While the US had lagged behind many other nations concerning airpower development through WW1, American political leaders took policy action in the 1920s and 1930s to put America at the forefront of aviation. In 1925, the US government created the Army Air Corps (AAC), which served as a branch within the US Army dedicated to airpower. Rather than developing airpower to meet the high expectations of many, however, the AAC focused nearly exclusively on developing and utilizing aircraft for close air support of troops rather than on the grand, rather than on performing the combat-altering role that many envisioned.[121] Even this effort, however, did little to bolster the aircraft's role in conventional combat.

Congressional testimony in 1934 by several General officers from the US Army indicates a lack of clarity over the mission of the AAC and inadequate preparedness overall for the air service. US Army Major General Drum stated in his testimony that the AAC had a total of 1,684 planes in 1933, yet only 191 were combat-ready aircraft adequately equipped with radios, bomb pylons, and other essential combat equipment.[122] This shortfall existed despite the fact that the AAC had spent 828 million dollars on aircraft development and procurement from 1920 to 1933. In short, the late 1920s and early 1930s produced little empirical evidence to support the

[121] Collier, Basic. *A History of Air Power.* London: Weidenfeld and Nicolson. 1974: 93.
[122] US War Department. *Testimony Before The Special Committee on Army Air Corps.* Washington DC: Columbian Building. May 21, 1934: 2865. US Air Force Archives Call 167.66-1.

perceptions of fear and optimism that pervaded many echelons of public and political life regarding the burgeoning air domain.

As my theory dictates, fear is created and sustained without empirical evidence because of the obfuscation between the offense and defense. Other weapons, such as tanks or ground soldiers, can indeed be used effectively for both offensive and defensive missions. The difference is the speed at which military leaders can transition the weapons from defensive to offensive tasks. Tanks and ground soldiers stationed in defensive postures require much logistical planning and support before they can be employed offensively. The time and logistical support they require means other states can use their intelligence apparatus to detect these changes and prepare for impending attacks.

Aircraft changed this calculus because planes taking to the air for defensive missions could easily transition to offensive attacks with little or no warning to other states. Efforts by the US government in the mid-to-late 1930s to develop the B-17 bomber showcase this problem. The long-range B-17 bomber was not sold to the American public as a weapon for offensive attacks against US adversaries. Instead, leaders told the public that the bombers were required for coastal patrols that could effectively sink any invading armada that would try its luck with an attack on the US coast. Even this opinion, however, was not held by everyone within the military. US Army Brigadier General Kilbourne stated in 1934 that the Air Corps could not protect America, and that "those believing in such a defense are lacking in powers of analysis and in judgment."[123] The British military agreed with such perceptions, noting in a 1932 report that "it is utterly impossible to stop hostile aircraft crossing a given line for the reason that the

[123] US War Department. *Testimony Before The Special Committee on Army Air Corps.* Washington DC: Columbian Building. May 22, 1934: 2974. US Air Force Archives Call 167.66-1.

sky is too vast to defend effectively."[124] Despite the difference of opinions among military and political leaders, efforts began a few years later to prove the defensive worthiness of aircraft.

In 1937, President Roosevelt ordered a fleet of B-17s to undertake an exercise where they were to locate a US battleship several hundred miles off the west coast. The bombers were able to locate the ship and 'sink' it with mock attacks utilizing harmless water bombs.[125] The following year, another group of B-17s intercepted the Italian liner *Rex* over 600 miles off the US coast in what was a widely publicized event designed to showcase the defensive applications of the bombers.[126] Major Curtis LeMay of the US Army Air Corps led both of these training missions. In a bit of irony that perfectly demonstrates how a lack of clarity between the defense and the offense causes fear, LeMay would later command a massive fleet of these bombers in WW2 that killed and wounded hundreds of thousands of Japanese soldiers and civilians with incendiary bombs and nuclear weapons.

The bombers the US developed in the 1930s for defensive purposes were easily transitioned into highly offensive roles just a few years later in both the Pacific and European theaters. The inability for other states to distinguish the exact purpose of aircraft during these early years of the air domain caused fear because states had to assume worst-case scenarios when crafting foreign policy to deal with a country that was building an air force. There was no empirical evidence up to the start of WW2, however, that the aircraft could indeed destroy large cities in short order, or cause entire economies to collapse with strategic bombing as Thomas Edison and many others had stated they could. Instead, these fears existed sans empirical

[124] British Royal Air Force. *G-2 Report 32525 – The Role of Aircraft in War.* M.A. London: July 16, 1932: 5. Air Force Archives Call 248.211-63.
[125] Sherry, Michael. 1987: 61.
[126] Copp, DeWitt. *A Few Great Captains: The Men and Events that Shaped the Development of U.S. Air Power.* Garden City, NY: Doubleday. 1980:

evidence because there was no clear delineation between the offense and the defense for aircraft in the early days of the air domain.

The Early Air Domain - Conclusion

The optimism for the early air domain I have identified thus far was prevalent before the airplane had proven its worth in battle because of the prevailing belief in the offensive efficacy that the airplane brought to the battlefield. This belief did not exist because empirical data proved the aircraft could level cities, cripple economies, or bomb the morale out of a population as many presumed. Instead, people believed in the offensive efficacy of the airplane for two reasons.

First, aircraft offered a new tool that could effectively cut across time and space in a manner that no other weapon at the time could. The airplane could easily bypass vast mountain ranges that made offensive land invasions nearly impossible. The aircraft could overfly the oceans that once offered significant protection to states like America, Great Britain, and Italy with relative ease. Targets behind enemy lines in combat that were once impossible to reach with artillery or ground soldiers were now within reach for bomb-laden aircraft.

During WW1, General Sir Hugh Trenchard of the British flying corps worked tirelessly to acquire bombers that could reach targets beyond enemy lines. Trenchard and other military leaders believed using aircraft to bomb targets that were behind enemy lines, like civilian populations, industrial facilities, and lines of communication, would quickly "blast Germany out of the war."[127] While aircraft did not blast Germany out of the war and ultimately played little role in the eventual outcome of WW1, the ability for the airplane to strike at targets that were unto this point out of reach fueled great optimism. Orville Wright even mused at the end of

[127] Doughty, Robert et al. *Warfare in the Western World – Vol II – Military Operations Since 1871*. Lexington, MA: D.C. Heath and Company. 1996: 581.

WW1 that "the aeroplane has made war so terrible that I do not believe any country will again care to start a war."[128]

In 1921, Italian soldier and air power theorist Giulio Douhet premised that an air force with 1,000 planes could strike at "every locality" within a defended enemy state and would constitute an "offensive capacity the like of which has never before been imagined."[129] The tantalizing prospect of a weapon that suddenly opened up targets beyond the reach of conventional forces created prevailing beliefs in the offensive efficacy of the new domain. In 1917, the New York Times bolstered this notion, opining that "The land may be trenched and mined; guns and bayonets form an impossible barrier. The sea may be mined and netted and the submarine lurks in its depths. The highways of the air are free lanes, unconquered as yet by any nation. America's great opportunity lies before her. The road to Berlin lies through the air. The eagle must end this war."[130]

This perception continued in the following years and extended into military education. In 1936, the Air Corps Tactical School (ACTS) in Montgomery Alabama taught military students that an air force was "at liberty to proceed directly to the ultimate aim in war: overthrow of the enemy will to resist through the destruction of those vital elements upon which modern social life is dependent."[131] The targets ACTS leaders envisioned that would cause political leaders and civilians to capitulate if attacked during conflict included transportation, steel and iron ore production, lines of communication, population centers, and power facilities,

[128] McFarland, Marvin ed. *The Papers of Wilbur and Orville Wright – Vol II – 1906-1948.* New York, NY: McGraw-Hill Book Company. 1953: 1121.
[129] Douhet, Giulio. 1921: 199-200.
[130] Sherry, Michael. 1987: 17-18
[131] Clodfelter, Mark. *The Limits of Air Power – The American Bombing of North Vietnam.* Lincoln, NE: University of Nebraska Press. 2006: 2.

The second reason people believed in the offensive efficacy of the airplane is a mirror image of why people felt so much fear for aircraft. That is the feeling that adequate defenses against aircraft were nearly impossible. Leading up to the start of WW1, the German military had the most advanced air defense units on the European continent. However, even their program was extremely limited in scope, with historian Edward Westermann noting that the "German experience with ground-based air defenses prior to the war advanced little beyond theoretical discussion and limited trials" with artillery designed to down enemy aircraft.[132] Other states fared worst in their advancement of air defense programs. As of Britain's entrance into WW1, there existed no organization within the British military designed to defend against aerial attacks.[133]

Britain's abdication of air defense investment going into WW1 is a strong indication of the lack of faith states held about air defenses because the British felt particularly vulnerable to the aircraft. The ability of an enemy air force to overfly the water around the island nation that had offered so much protection in the past created much unease within Britain. Despite feeling particularly vulnerable to aerial attacks, the British made virtually no effort to develop aircraft defense organizations leading up to WW1. While there is no single reason researchers have identified to explain this lapse in military preparedness, the most likely reason stems from the perception during this period that there was little a state could do to defend against a mass of aircraft sent to bomb the nation. The belief in the effectiveness of the offense and the ineffectiveness of the defense directly caused the optimism many held during this period for the aircraft to radically alter war for the country that best utilized the new air domain.

---

[132] Westermann, Edward. *Flak: German Anti-Aircraft Defenses, 1914-1945.* Lawrence, KS: University Press of Kansas. 2001:15.
[133] Routledge, N.W. *History of the Royal Regiment of Artillery: Anti-aircraft Artillery, 1914-55*. London: Brassey's. 1994:3

From 1903 to 1939, civilians and elites expected airpower to win future wars for their nation, and they feared adversarial aerial attacks. Both of these perceptions existed before there was empirical evidence to support such opinions. The first combat data from the early airplane came as WW1 began and gave only small glimpses into the defensive capability of aircraft. During the first weeks of World War 1, pilots proved themselves useful only as information gatherers. At times this intelligence was vital to a given battle, such as when information gleaned by aviators played a significant role in the German destruction of the Russian Second Army at Tannenberg in August 1914.[134] However, many of these early missions were simple scouting missions designed to gather intelligence to bolster an army's defensive posture. While early aircraft primarily functioned in defensive roles, technological developments quickly allowed militaries to lade their aircraft with munitions and guns that helped transition the airplane into an offensive weapon.

By 1917, aircraft were attacking cities with simple munitions with "almost commonplace occurrence."[135] Nevertheless, the early transition into the offensive role that many believed the aircraft was fully capable of performing was vastly ineffective during WW1. Historical reports from WW1 show that the airplane made little-to-no difference in the outcome of most battles. Even without empirics to ground the perceptions of fear and optimism, however, scholars, elites, and laypeople alike bought into the notion that the airplane was "the offensive weapon par excellence" during the early days of airpower.[136]

As my research shows, fear for the early air domain existed because of the inability for states to discriminate between the offensive or defensive purpose of another state's air force. During the first part of the early air domain examined (1903 – 1915), fear existed because there

[134] Kennett, Lee. *The First Air War – 1914 - 1918.* New York. Simon and Schuster, 1991: 31.
[135] Kennett, Lee. 1991: 55.
[136] Douhet, Giulio. 1921/2009: 15.

was no explicit offensive or defensive role for the aircraft. Early uses of the aircraft in defensive missions added little more to the battlefield than the dirigibles and balloons used by nations for years before the invention of powered flight. Efforts to employ the airplane in offensive roles also proved ineffective due to the limited accuracy of airdropped weapons and underpowered aircraft that could carry only small munitions. While there was wild speculation about the airplane's capabilities in both forms of combat, the actual performance of the aircraft up to 1918 left many wondering what its real role in future combat would be. Just as Jervis asserts with a new weapon, this caused anxiety among elites and the public because there was no practical way for states to prepare for a weapon that held such potential, yet did not have a clear and distinguishable role in combat.

Post WW1, aircraft began to demonstrate their ability to perform both offensive and defensive missions with effectiveness. Advances in aerial munitions, bombing sites, and Mitchell's test attacks on ships and submarines helped develop aircraft into the offensive weapons that early airpower advocates had proclaimed they were. Defensive missions also became more effective as technology progressed. Wireless radios allowed pilots to communicate enemy advances quickly, and longer-range aircraft allowed pilots to patrol at great distances. Increases in loitering times also allowed pilots to stay airborne longer and gather the intelligence required for adequate defenses against impending attacks.

The dual-role nature of aircraft during this period, such as bombers that could be used for coastal defense or to attack another state, caused fear and anxiety because leaders could not discern the true intentions of a state building up an air force. The aircraft quickly became a gray weapon that could execute either mission in short order.

Optimism for aircraft to become a panacea for conventional conflict during this period arose from the prevailing belief that aircraft brought extensive offensive capabilities to a state that developed the technology correctly. This belief ran rampant among famous authors like H.G. Wells, to early airpower inventors like the Wright Brothers, to acclaimed scientists like Thomas Edison. Political leaders bought into the idea as well, with the appropriation of ever-growing budgets designed to grow robust and independent air forces. During WW2, the US alone built as many as 95,000 aircraft per year to seize the offensive advantage and win the war.[137]

While outside the period under investigation for this chapter, this pervasive belief in the efficacy of aerial offense continued unabated for decades to come. Military leaders based the Allied Combined Bomber Offensive (CBO) in the European theater, and the US bombing campaign against Japan during WW2, on the perception that strategic aerial bombing against the correct targets would cause "wholesale administrative, psychological, and economic breakdown, cracking the backbone of the enemy's will to resist."[138] This optimism was birthed and grew after Kitty Hawk because of widespread belief in the aircraft's offensive efficacy, even before evidence existed to support such beliefs.

The Cyber Domain: 1986 to 1998

There is no clearly defined beginning for the cyber domain. As noted earlier, I rely on cyber researcher Jeff Healey's assertion that 1986 is the beginning of cyber conflict and mature debates about the cyber domain. Before 1986, there were undoubtedly feelings of fear and optimism, and discussions were taking place regarding the new domain at the highest levels of government. Reports from the early 1980s indicated that Pentagon 'tiger teams' could always

[137] Smithsonian Air and Space Museum. *300,000 Airplanes.* May 2007. https://www.airspacemag.com/history-of-flight/300000-airplanes-17122703/ (accessed Nov 2, 2018).
[138] Pape, Robert. *Bombing to Win – Air Power and Coercion in War*. Ithaca, NY: Cornell University Press. 1996: 92.

break into US military networks when asked to do so, which spurred debates about US military network security.[139] While cyber security was quickly becoming an issue, there was no significant event in the early 1980s that spurred higher debates about the cyber domain and network security.

With only low-level cyber activity ongoing at the time, cyber debates were embryonic and often produced rather senseless recommendations. One such proposal, from Joseph Coates in the early 1980s, recommended setting an IQ ceiling for computer operators so that nobody too smart ever took advantage of the vulnerabilities within the systems.[140] As Healey notes of the early 1980s, "all the elements were in place for cyber conflict: a foundation of large-scale computer networks, a new conception of computer security, and the first glimmers of national security challenges. Nevertheless, it took two malicious cyber incidents in the mid-to-late 1980s to launch the cyber phase that Healey calls "Realization," which began the age of cyber conflict.[141]

The first of the two large cyber operations took place in 1986 when a team of German hackers undertook a cyber attack designed to steal information related to President Reagan's Strategic Defense Initiative (SDI - i.e., Star Wars) from several US research facilities. The objective of the attack, nicknamed Cuckoo's Egg by US government officials, was to find information that Soviet KGB officials would be willing to buy. American officials eventually arrested the hackers and sentenced them to prison. While the attack did little to spur organizational or policy change within the burgeoning global cyber enterprise and had no

[139] Orr, Kelly. "Pentagon Computers: How Vulnerable to Spies?" *US News and World Report.* October 31, 1983. 36-37.
[140] Graham, David, and Ulrike Richardson. *Computer Crime and Security: An Annotated Bibliography of the Periodical Literature.* GAO Report. GAO: Washington, DC. 1984: 3.
[141] Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* USA: CCSA. 2013:29.

meaningful impact on the SDI program, it did help set into motion the causal mechanisms I identify in my theory for fear and optimism in a new domain.

First, the Cuckoo's Egg attack was discovered and exposed by Cliff Stoll, a former astronomer who had changed careers to become a computer system administrator. Stoll discovered the attack when he began investigating a 75 cent billing discrepancy he noticed within a government computer system. After much investigation, Stoll discovered the theft of the SDI data and promptly alerted officials to the break-in. Far from causing alarm within the US government, however, Stoll received little support from any government agency for the investigation.

From the events of Cuckoo's Egg, we find the first real evidence of the faith people placed in the offense and lack of belief in the defense. When the hackers were eventually arrested and put on trial, the US government did not even send any government experts to testify about the extent of the damage caused by the attack.[142] The ability for 'tiger teams' to 'always' break into government networks, like reports in the early 1980s had shown, likely numbed government officials to any real attempt at defense-through-prosecution of hackers, as evidenced by the lack support for Stoll's investigation or the court case. Further, it is tough to quantify the value of information stolen as part of an offensive cyber attack. Offensive cyber attacks can gather precious information for the state that sponsors the attack, but the victim has a hard time quantifying that value, meaning prosecution is difficult as Stoll learned.

In 1988, Stoll succinctly summed up the budding belief in the efficacy of the offense when he stated that offensive cyber operations "can be cost-efficient, offer nearly immediate results, and target specific location" and are "insulated from risks of internationally embarrassing

[142] Healey, Jason. 2013: 30.

incidents."[143] Just as with the early air domain, this belief in the offense would provide the basis for the growing optimism held by elites and the public to alter future conflicts, even before empirical evidence existed to support such perceptions.

The next sizeable cyber attack, the Morris Worm event of 1988, trigged fear among the public and elites because, as stipulated in the theory, the true intentions of the attack were nearly indistinguishable during the early stages of the attack. Unlike Cuckoo's Egg, the Morris Worm was launched by foreign agents, but as a scientific experiment by a graduate student at Cornell. The purpose of the computer code, created and implemented by Robert Morris of Cornell's computer science program, was designed to cause UNIX connected computers to send a message to Morris so he could create an accurate count of devices on the internet. Up to this point, there was no accurate count of the number of computers connected to the internet. Either by oversight or by design (some believe Morris intentionally designed the code to be malicious), the program began replicating itself and quickly clogged the limited bandwidth available for emails and other data transfer programs. Within 12 hours of its release, the Morris Worm had bogged many Unix-based computers down so severely that only a small percentage of traffic could make it across the nascent internet.[144]

As with the Cuckoo's Egg attack, the US Government had a difficult time calculating the amount of damage caused by the Morris Worm. A 1989 US Government report presented to Congress estimated the cost from the Morris Worm, which took only two days to eradicate, at between $10,000 and $10,000,000, an incredible range covering two orders of magnitude.[145] The ease with which a college student could cause such a massive slowdown in the growing

[143] Healey, Jason. 2013: 30.
[144] The IEEE Computer Society. "The Morris Worm: A Fifteen-Year Perspective." *IEEE Security and Privacy*. 2003: 35
[145] US General Accounting Office. *Computer Security – Virus Highlights Need for Improved Internet Management.* Report to Congress. Washington, DC: US GAO. 1989: 17.

internet and the inability for the government or corporations to assess the damage accurately further heightened the belief in the offense and the weakness of cyber defenses. While the Morris worm would seem to provide some empirical evidence of the power of cyber attacks, it is essential to remember the worm took only two days to remove from computers, and thus proved nothing of cyber's ability to alter interstate conflict or cause political change among state leaders.

In response to the Morris Worm and other smaller cyber attacks that occurred shortly after that, computer security expert Winn Schwartau testified before Congress in 1991 that "government and commercial computer systems are so poorly protected today that they can essentially be considered defenseless; essentially, an electronic Pearl Harbor waiting to occur."[146] Schwartau's assessment was backed up in a 1991 National Research Council report that highlighted why the offense had so much potential in the new domain, and why defense was so difficult: the proliferation of computers into all segments of society, poor US Government policy to regulate the industry, inadequate hardware and software design, little-to-no use of basic security protocols by users, and little public awareness of the threat. The report stated that these conditions created a cyber domain where there were "few incentives to make system[s] more secure" and where network security did not increase "at a rate fast enough to match the apparent growth in threats to systems."[147] Empirical evidence would back this up, as a 1994 US Army War College research paper noted that the US government only detected two percent (3,600) of the estimated 182,000 attacks on its networks from June 1993 to July 1994.[148]

[146] US Congress. "Hearing Before the Subcommittee on Technology and Competitiveness." *Computer Security.* Washington, DC: Government Printing Office. 1991: 10.
[147] National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press. 1991:3.
[148] Fredericks, Brian. *Information Warfare: The Organizational Dimension.* Thesis. Carlisle Barracks, PA: US Army War College. 1996: 5.

As outlined in the theory in Chapter One, belief in the offense in the early days of the cyber domain caused great optimism among government officials for the domain's ability to influence future conflict. Just as H.G. Wells and other authors wrote influential books about the role of airpower during the birth of the air domain, so too did authors theorize about the influence of the cyber domain on future conflict. Prominent books in the 1990s, like Schwartau's (1994) *Information Warfare*, and Alvin and Heidi Toffler's (1995) *War and Anti-War* made grand claims about the cyber domain's ability to influence future conflict outcomes. Noted scholars like John Arquilla (1994) also wrote about the strategic implications of information warfare and its dominance over traditional strategies of attrition and conventional maneuvers.

Optimism for the cyber domain's ability to fundamentally alter war was not limited to scholars and academics, however. In 1995, US Air Force Secretary Sheila Widnall and Chief of Staff General Ronald Fogleman published *Cornerstones of Information Warfare,* which detailed the domain's role in future wars. In the work, the authors state, "Information has its own characteristics of mass, motion, and topography… There are strong conceptual parallels between conceiving of air and information as realms. Before the Wright brothers, the air, while it obviously existed, was not a realm suitable for practical, widespread military operations. Similarly, information existed before the Information Age, but the Information Age changed the information realm's characteristics so that widespread operations became practical."[149] The authors also believed that utilizing the cyber domain had "become central to the way nations fight wars" and that "information technology advances will make dramatic changes in how this

[149] Fogleman, Ronald and Sheila Widnall. *Cornerstones of Information Warfare.* 1995. http://www.c4i.org/cornerstones.html (accessed November 14, 2018)

nation fights wars in the future."[150] As with the early air domain, optimism for the cyber domain's ability to alter future conflict existed without empirical evidence to support such beliefs. While events like the Morris Worm did cause some issues, it was also eradicated quickly after its release with no lingering effects.

As with the early air domain, the inability to distinguish between the offense and the defense caused fear for the early cyber domain. The Morris Worm is a perfect example of how difficult it is to distinguish the intentions of cyber activities. In the aftermath of the Morris Worm attack, Morris's father, then a computer expert with the National Security Agency (NSA), said that "It's perfectly honest to say that there is not a fraudulent or dishonest bone in [his son's] body."[151] Still, others disagreed, feeling that Morris had created his program with ill intentions. US government officials said that "Mr. Morris's sole intention was the break into as many computers in the United States as he could" to cause damage and chaos.[152] This inability for people to discern offensive intentions from defensive ones in the cyber domain, just as with LeMay's fleet of bombers in the 1930s, caused fear among the public and elites.

Lieutenant Colonel Rhoads, the first commander of the US military's first cyber unit (609th Information Warfare Squadron), discussed the blurred lines between the offense and the defense during his tenure as commander of the 609th in the mid-1990s. In the early days of his squadron, he placed offensive cyber operators alongside defensive personnel. When offensive operators began an attack on an adversary, the defensive operators could gather intelligence based on how the enemy reacted. Rhoads notes that this is an "unfortunate way to get

[150] Fogleman, Ronald and Sheila Widnall. 1995.
[151] Markoff, John. *Computer Intruder is Found Guilty.* January 23, 1990. https://www.nytimes.com/1990/01/23/us/computer-intruder-is-found-guilty.html (accessed November 12, 2018)
[152] Markoff, John. January 23, 1990.

intelligence," but notes it was an effective way to glean the required information.[153] As outlined in the theory, strong cyber defenses rely on accurate intelligence about an adversary's capabilities, and offensive cyber attacks are a preferred method to acquire the information.

The blurred line between offensive and defensive cyber operations does not exist in the same way for other conventional instruments of war like tanks, soldiers, and battleships. Detectable movements and other signals that would identify an impending offensive attack usually precede any offensive use of these conventional weapons. A state with a functioning intelligence apparatus would detect some or all of these signals and could produce an initial assessment of the other state's intentions. Without these signals, cyber attack victims do not know if a cyber attack is a simple intelligence gathering operations, or a serious attempt to disable vital networks and computer systems. The growing fear that this blurred line caused in the 1990s prompted action from the US government.

Cyber Domain 1998 - 2014

In 1998, President Clinton said the US government must enact policy to "swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[154] It is not clear what event if any, spurred President Clinton to enact such policies. Just a year earlier, in 1997, the Government Accountability Office (GAO) listed federal cyber assets for the first time on their "High Risk" list of government systems that needed immediate defense from attack.[155] The historical records also show that in February 1998, several months before Clinton's remarks, the Department of

[153] Healey, Jason. 2013: 40.
[154] Clinton, Bill. *PDD/NSC-63.* Presidential Decision Directive, Washington DC: White House. 1998: 2.
[155] Government Accountability Office. *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information*. 2017. https://www.gao.gov/highrisk/ensuring_the_security_federal_government_information_systems/why_did_study (accessed Nov 8, 2018)

Defense suffered a massive cyber attack that compromised hundreds of computers and networks at multiple military and government research locations. The three-week-long cyber attack, code-named Solar Sunrise, started shortly after tensions began to escalate in the Middle East. In January 1998, Iraq barred United Nations (U.N.) nuclear inspectors from accessing several military sites. President Clinton responded in February by sending several thousand additional combat troops to the region.

Solar Sunrise began in the first week of February and continued nearly unabated for weeks due to weak US cyber defenses. Government officials described the attack as "the most serious intrusion into the United States up to that point."[156] With the attacks happening against the backdrop of growing US/Iraq tensions, Deputy Defense Secretary Hamre briefed President Clinton that "the intrusions might be the first shots of a genuine cyber war, perhaps by Iraq".[157] Several weeks later, US investigators discovered the identity of the hackers that conducted Solar Sunrise: two 16-year-olds from Northern California and an 18-year-old living in Israel. The teenagers would later tell investigators they undertook the attack for fun.

Solar Sunrise highlighted the fragility of the nation's cyber systems and showed how difficult it was to pinpoint the source and intentions of a cyber attack. These problems were especially acute for Solar Sunrise because the attack happened during the military crisis unfolding in Iraq at the time. As asserted in the theory, this attack caused fear among government officials because of the inability to discern between offensive and defensive objectives and intentions. While Solar Sunrise was an offensive attack on US networks, the purpose of the attack was unclear to decision-makers. If government officials knew the identity of the attackers and their intentions when Solar Sunrise began, they would react differently than

[156] Healey, Jason. 2013: 122.
[157] Graham, Bradley. *U.S. Studies a New Threat: Cyber Attack.* Washington, DC, May 24, 1998.

if they had determined the attack was an offensive operation order by Saddam Hussein for nefarious purposes. In each case, the attack is going to appear nearly identical to political leaders in the beginning. While the attack did cause fear and consternation among government officials, the historical record shows it did not alter the political calculus of the US during the ongoing Iraq crisis.

Solar Sunrise also shows how my causal mechanism for optimism functioned. The ability of three teenagers to conduct such a massive offensive attack only furthered the belief among many decision-makers that the offense was, by far, the stronger form of warfare in the cyber domain. The belief in the offense was heightened again after testimony given in 1998 before Congress by seven Boston-based hackers who stated they could take down the entire internet in 30 minutes.[158] As described in the theory, the belief in the efficacy of the offense over the defense directly leads to optimism for the cyber domain to beneficially alter future conflict in the same way it did with early airpower, despite little empirical evidence that it can meaningfully change the outcome of wars.

When several teenagers can conduct such an attack of Solar Sunrise's magnitude, or when barely-trained pilots can overfly geographic boundaries or military defenses and bomb a city, as with the early air domain, the apparent efficacy of the offense fuels great optimism. This optimism persists even when there is no empirical evidence of the domain's capability to alter the political calculus of a state, to influence the outcome of a conflict, or, in an extreme case, to destroy a large city in five minutes or take down the entire internet in 30 minutes.

Cyber attacks of the late 1990s and early 2000s garnered much of the same responses as the previously discussed attacks. The Moonlight Maze attack, a long-term attack started in 1998,

[158] Timberg, Craig. *In 1998, these hackers said the internet would become a security disaster. Nobody listened.* June 27, 2015. https://www.dailyherald.com/article/20150627/business/150629234/ (accessed November 14, 2018)

left US government officials unable to determine intentions or motives for quite some time. While the US did eventually discover that the Russian government was behind the attacks, the vast array of targeted institutions (e.g., government agencies, private universities) gave no clear indication of the intentions of the attack other than general intelligence gathering. As is a theme with nearly all major cyber attacks since 1986, the attack caused fear among political leaders and the public but caused little political reaction from the US government. The US government responded to the attack by sending the Russian government a simple demarche demanding the phone numbers of the hackers. The Russian government replied to the demarche with a list of inoperative phone numbers.[159]

Fear over attacks like Moonlight Maze prompted US Government officials in the 2000s to create cyber policy based on worst-case scenarios. In 2007, Director of National Intelligence (DNI) Mike McConnell briefed President Bush on a hypothetical scenario: instead of terrorists flying aircraft into buildings on 9/11, they could simply break into the computer databases of several major financial organizations and erase the contents. McConnell told the president that erasing or corrupting just a portion of the information in these databanks would cause mass panic and entire economies to collapse for lack of confidence in financial transactions. "The economic effects of this attack," McConnell told the president, "would be worse than those of the physical attacks of 9/11."[160] Bush responded by telling McConnell and other advisors in the room that he wanted the US to undertake a cyber version of the Manhattan Project, alluding to the secret and costly WW2 project that built the atom bomb. The meeting resulted in a proposed 5-year $40 billion project that sought to expand US cyber capabilities vastly.[161]

[159] Healey, Jason. 2013: 49.
[160] Harris, Shane. 2014: 142.
[161] Harris, Shane. 2014: 143.

Only a few years later, Michael Hayden, who served as director of both the CIA and NSA, stated that powerful cyber weapons were "a new class of weapon, a weapon never before used" that hinted at a "whiff of August, 1945."[162] Just as many other political elites had done elsewhere, Hayden compared cyber weapons, which had zero attributed deaths and scant physical destruction on their resume, to that of nuclear weapons, which have proven their destructive capability by killing and injuring hundreds of thousands of people and leveling entire cities during the Second World War. This fear resulted from the inability of government officials to accurately ascertain the offensive or defensive nature of cyber events.

Further evidence of the blurred line between the offense and defense are comments made in October 2012 by then-Defense Secretary Leon Panetta. The Secretary told a group of business executives that a cyber attack "could be as destructive as the terrorist attack on 9/11" and he stressed the need for offensive cyber capabilities undertaken "in a manner that is consistent with the policy principles and legal frameworks" in order to protect the US.[163] The implications of the Defense Secretary's remarks are clear: offensive cyber operations are a requirement for strong cyber defense, meaning it is difficult-to-impossible to distinguish between the two. This type of posture causes fear among other states because they cannot discern the intentions of US cyber actions. I described this same process with the early air domain when Major LeMay sought a fleet of bombers for coastline defense in the 1930s. Yet just a few years later, LeMay utilized his contingent of bombers as powerful offensive weapons against Japan in WW2.

In the early 2010s, President Obama released cyber policies that further highlighted the blurred line between the offense and the defense. President Obama signed Presidential Policy Directive 20 (PPD-20) in 2013 that identified critical sectors of the nation that agencies needed

[162] Seabrook, "Network Insecurity," *The New Yorker*, 20 May 2013: 70.
[163] Farnsworth, Timothy. "U.S. Officials Detail Cyber Policy." *Arms Control Today*. 2012: 32-33.

to defend from cyber attacks. The report also detailed the roles and responsibilities of various government agencies concerning offensive cyber operations. While PPD-20 is classified, the White House later released an unclassified single-page fact sheet on PPD-20 after the full PPD-20 document was publically leaked. The fact sheet gives no specifics, but does note that PPD-20 is "part of the Administration's focus on cyber security as a top priority."[164]

Further, the fact sheet states that PPD-20 "establishes principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools we have at our disposal."[165] Elements of the fact sheet give the impression of burgeoning US involvement in offensive cyber operations, yet the conclusion states that network defense and law enforcement are the priority. Interestingly, the fact sheet notes that US policy shall be to undertake the least offensive cyber operations possible to mitigate cyber threats. This language provides further evidence that decision-makers view offensive cyber operations as necessary for strong cyber defenses, meaning the line between the offense and defense is unclear.

Beyond establishing guiding principles for cyber operations, Harris (2014) posits that PPD-20 transformed US cyber operations in a far more fundamental way because it elevated cyber operations to the same status as traditional combat domains.[166] The policy directive instructed US agencies to no longer treat the cyber domain as a support medium, but rather as an active arena for combat. Having the US government identify the cyber domain as an active combat medium would only serve to heighten fears and optimism because major powers can help create and maintain international norms by giving legitimacy to a given behavior or idea. With PPD-20, the US government made a clear case that offensive and defensive cyber operations are legitimate combat operations, meaning the US can undertake them as required for national

[164] White House. *Fact Sheet on Presidential Policy Directive 20.* Fact Sheet, Washington DC: White House, 2013.
[165] White House. 2013.
[166] Harris, Shane. *@War*. New York, NY: Houghton Mifflin Harcourt Publishing. 2014:56.

defense. Interestingly, acknowledging the cyber domain's status as an active combat domain is precisely what the US Air Force's document *Cornerstones of Information Warfare* did nearly 20 years early.

Some scholars felt that it was not wise for political leaders to suggest that offensive cyber operations were an effective means of solving cyber defensive problems. Martin Libicki, then working as a senior scientist at the RAND Corporation, wrote in 2011 that "a state with nuclear weapons that is worried largely about the survival of the nation and its citizens can afford to ignore whatever relative superiority its rivals may enjoy in cyberspace."[167] Libicki asserted that policymakers need not undertake offensive cyber operations to provide better national security and that this notion has "little basis in theory or fact."[168]

One of the prime reasons Libicki and others tried to persuade leaders against such positions is because "states have little knowledge of exactly what [cyber] weapons are in the arsenal of their rivals" and thus states concerned about cyber stability should focus only on defensive measures.[169] While some aspects of the argument have merit, Libicki never addresses the belief espoused by many government leaders that states can only construct effective cyber defenses if they have some working knowledge of the offensive cyber tools that an adversary may employ. Such a requirement necessitates gathering accurate intelligence on an adversary, and offensive cyber tools had emerged as a favored method for intelligence agencies because of their effectiveness and relatively low risk.

A 2014 National Academy of Sciences report on cyber security highlighted this blurred line between the offense and defense. The authors of the report note that the US promotes cyber

[167] Libicki, Martin. "The Nature of Strategic Instability in Cyberspace." *The Brown Journal of World Affairs*. 2011: 72.
[168] Libicki, Martin. 2011: 77.
[169] Libicki, Martin. 2011: 77.

defense on the international stage every chance it gets, yet sends mixed messages to fellow states because the US consistently undertakes offensive cyber operations designed for "intelligence purposes" that can be used to strengthen cyber defenses.[170]

During this period, some researchers and decision-makers took the opposite stance and felt the increasing use of offensive cyber operations for defensive purposes was a tack in the right direction. Keith Alexander, writing in 2013 as the director of the National Security Agency (NSA) and commander of US Cyber Command (USCYBERCOM), stated that the US had developed "an evolving set of capabilities and activities that have not yet reached their collective potential."[171] While Alexander touted the need for strong offensive capabilities, he always couched his argument in defensive terms (Alexander's journal article from which this citation comes from is title ***Defending*** *American in Cyberspace* – the emphasis is mine*).* The approach of justifying offensive cyber operations as a cornerstone of strong cyber defenses sustains the blurred line between the offense and the defense in the cyber domain and fuels the fear we observe today despite limited empirical evidence to support such perceptions.

From another state's perspective, Alexander's statements prove problematic because a simple cyber operation designed to gather intelligence and a sophisticated operation designed to paralyze a critical network (e.g., financial systems, electric grids) can both initially appear identical to the targeted state. Both require computer experts to hack into the target state's networks and computers via a vulnerability within the system or through brute force hacking. The first identifiable difference between the two operations is what the hackers do once inside the network. If the mission is intelligence gathering in nature, the cyber operators will search for the desired information until they acquire it, or they lose access to the network. If their intent is

[170] National Research Council. *At the Nexus of Cybersecurity and Public Policy.* Policy Report, Washington DC: National Research Council. 2014: 104-105.
[171] Alexander, Keith. "Defending American in Cyberspace. *The National Interest.* 2013: 18.

nefarious, the hackers will utilize their network access to upload code designed to degrade the system they are targeting.

In each case, the initial entry into the targeted state's network appears to the victim very much like Lemay's fleet of bombers in the 1930s would have seemed to adversaries. That is, the weapon's offensive or defensive purpose is nearly indistinguishable to intended targets until it is employed. Because of this, adversaries fear the simple existence of the weapon in their counterpart's inventory because its offensive or defensive use is indiscernible until utilized. Fear and a negative security spiral follow as states posture their forces for worst-case scenarios, just as President Bush and Director McConnell did in the mid-2000s.

The Stuxnet attack of the early 2010s is one of the only cyber events that appeared overwhelmingly offensive because it caused physical damage for the victim. The attack, purported orchestrated by the US and Israel, was part of a covert operation designed to delay and deter the Iranian government from developing nuclear weapons. The Stuxnet virus began surgically infecting Iranian computer systems at the Natanz nuclear plant sometime around 2010. The virus rapidly altered the speed of Iranian P-1 nuclear enrichment centrifuges and caused premature failure of the components. At the same time, the virus modified the display information to local technicians to mask the oscillations. The goal of the attack was to slow down Iranian enrichment by causing premature failure of the centrifuges with the hope that Iranian technicians would struggle to fix what appeared to be regular industrial component failures.[172] The interesting aspect of the Stuxnet attack is that while it is the most offensive use of cyber weapons to date, experts disagree on its offensive usefulness.

[172] Valeriano, Brandon and Ryan Maness. 2015: 152.

The computer security company Kaspersky Labs suggested that the Stuxnet attack set Iranian nuclear efforts back by five years.[173] The US intelligence community estimated the attack cost Iran approximately two years,[174] while the International Atomic Energy Association (IAEA) suggested that the attack cost Iran no time as they sped up production on uninfected centrifuges.[175] Others have also suggested that the attack may have helped the Iranians because it spurred them to replace the aging P-1 centrifuge with more reliable components.[176]

The striking aspect of the debate over the effects of Stuxnet is that after news broke of the attack, experts heralded it as "the cyber equivalent of dropping the atom bomb"[177] and a "new era in warfare."[178] However, even this advanced cyber attack gave no clear indication of cyber's offensive efficacy, and it gave no empirical evidence to support the hyperbole and fear outlined earlier. While Stuxnet certainly had some impact on Iran's nuclear program, the evidence available shows that even the most sophisticated cyber attack undertaken to date showed little ability to cause the catastrophic damage many experts believed cyber weapons could inflict. So while belief in cyber's offensive efficacy continues unabated, there is little empirical evidence to support such beliefs.

Conclusion

The early air domain and the modern cyber domain exhibit nearly no similarities on the surface, yet we find many similarities regarding perception development during their initial growth stages. The two perception similarities investigated in this chapter are the widespread

[173] Barsashka, Ivanka. 2013. "Are Cyber Weapons Effective?" *The RUSI Journal* 158: 49.
[174] Sanger, David. 2012b. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* Random House, New York. 2012206.
[175] Sanger, David. 2012b: 206.
[176] Sanger, David. *The Reckoning: How President Obama Has Changed the Force of American Power.* Crown Publishing, New York. 2012a: 188.
[177] Broad, William, John Markoff, and David Sanger. "Israel Tests on Work Called Crucial in Iran Nuclear Delay." *NY Times* (NY Times), 15 January 2011.
[178] Clayton, Mark. "The New Cyber Arms Race." *Christian Science Monitor*, 7 March 2011.

fear and optimism for each domain before any empirical evidence was available to support these perceptions. The optimism for early airpower and modern cyber power to alter future conflicts played a significant role in foreign policy between states in the early years of each domain, yet to date, scholars have not identified the source of this optimism. The most widely theorized source of this optimism is rhetoric from 'experts' who focused on what was technically possible in each domain, rather than what is realistically feasible. Early airpower advocates spoke of destroying large cities in minutes or crippling economies even before aircraft could carry useable munitions or bombing sites could produce semi-accurate hits. Similarly, cyber power prophets spoke of the ability to ruin economies or disable vital social networks even before any empirical evidence existed that such a feat was possible. A prime example is US Senator Joe Lieberman's (I-CT) statement in 2012 that offensive cyber weapons could "paralyze [a] nation with targeted cyber attacks on critical networks" and that such belief is "anything but hype."[179]

As with optimism, fear for the early air domain and the modern cyber domain were created and sustained without empirical evidence. This fear drove states to enact policies and shift budgetary resources even before evidence showed that national defense required such changes. One of the most popular explanations for this is the suggestion that this fear stems from experts who scare people into believing the hype about the domain's ability to inflict damage on society. As discussed in Chapter One, this premise is flawed because such expert rhetoric has not produced the same inflated fear that we see for other forms of conflict like terrorism.

The theory outlined in the previous chapter predicts that this fear is the result of the inability of states to accurately distinguish between the offensive and defensive purposes of cyber capabilities. Just as with the early air domain where a growing air force in one country could easily and quickly be used for either defensive or offensive mission, so too does growing

[179] Quigley, Kevin, Calvin Burns, and Kristen Stallard. 2015: 113.

cyber capabilities cause fear because states cannot discern the purpose of another state's growing cyber arsenal. Two factors intensify this fear. First, offensive cyber attacks are a preferred method to glean the intelligence required to bolster a state's cyber defenses. States desiring strong cyber defenses must then develop viable offensive cyber capabilities to gather data needed to fortify their defenses. Second, the methods and techniques required to penetrate another state's networks to gather this intelligence are nearly identical to operations a state would undertake to launch an offensive cyber attack. Each requires network access through vulnerabilities or brute force methods. For the attacked nation, it is nearly impossible to determine whether the intruder intends to probe for intelligence or to cause damage.

Up to the present, we find that the perceptions about the modern cyber domain are developing much the same way as the early air domain. There is great optimism for the cyber domain to alter future conflict by 'overflying' traditional barriers to force employment, just as with the early airplane. Yet, as I show for the periods of each domain that I researched, this optimism was/is not empirically supported. I theorize that this optimism exists because of the overwhelming belief in the offensive efficacy of cyber weapons. The belief in cyber's ability to bypass traditional defenses and penetrate enemy networks that control vital aspects of economic, military, and social life is identical to the belief in the early airplane and causes great optimism. Fear over the two domains existed/exists without empirical evidence to support this perception because the unique characteristics of the two domains made/make it nearly impossible for states to distinguish between offensive and defensive activities. The established tenets from IR scholarship on which my theory rests illustrate how this causes the fear we observe today, even without data that says it is warranted. In the next chapter, I test these theoretical propositions with a survey experiment to further determine their validity.

CHAPTER 3

SURVEY EXPERIMENT ANALYSIS AND DISCUSSION

Description of the Survey Experiment

The survey experiment employed for this research project more clearly illuminates causal mechanisms at work in perceptions of fear and optimism in the cyber domain when compared to cyber research that relies upon aggregate-level cyber data or public polling (Lewis 2013; McGraw 2013; Rid and McBurney 2012; and Singer and Friedman 2014). The survey experiment analyzed in this chapter creates specific control and treatment scenarios and randomizes respondents into each scenario to provide firmer support for the theory because the treatment is the only difference between scenarios. This, along with randomization, eliminates other factors that may be influencing respondent selections and instills greater confidence in the findings. To date, this is the first known cyber research that utilizes a survey experiment to verify theory validity.

Before beginning the survey experiment portion, respondents answered five demographic questions – age, gender, education level, household income, and left/right ideology. These provide enough information to meet the goals of demographic questions as set forth by Hughes, Camden and Yangchen (2016). I conduct the experiment on two survey pools. First is a public pool of approximately 1,000 US residents. The second is a group of 64 people within the US government who have above average knowledge of the cyber domain. This allows a test of the theory at both the public and expert level to determine if responses to the treatments in the survey experiment influence the populations differently. Determining any difference between

the groups is essential because these experts are relatively similar (e.g. age, education, experience) to those who advise policymakers and help formulate cyber strategy.

Description of the Public Survey Population

The survey was conducted under the University of Georgia's Institutional Review Board approval STUDY00006790. I recruited the respondents via Amazon's MTurk service with three pre-screening requirements: (1) having a US IP address, (2) at least 500 previously completed Human Interface Tasks (HITs), and (3) a previous HIT approval rating of 99 or greater. The recruitment process yielded 1,023 competed surveys. Of those, 24 respondents never completed the entire survey (percentage completed ranged from 3 percent to 96 percent), and thus were deleted before running any statistical analysis.

The advertised estimated completion time for the survey was listed as 3 to 5 minutes on the MTurk recruitment page. Reading the entire survey at a reasonable pace and responding to the answers after ten seconds of decision time generally yielded a completion time of approximately 3 minutes during pre-testing. Reading the survey at a rapid pace and answering the questions with minimal decision time generally yielded completion times of 1 minute and 15 seconds to 1 minute and 30 seconds. With a desire to only analyze respondents that adequately read and understood the survey experiment, I deleted data from respondents with a completion time of less than 1 minute and 10 seconds from the dataset. Twelve respondents met this criteria, leaving 987 respondents. Of these, the average completion time for the survey was 5 minutes and 48 seconds. This number is higher than pretesting indicated the survey would take because respondents were given several hours to complete the survey in MTurk before the system would time them out. Multiple respondents had excessive completion times (the highest being 270

minutes), likely due to the need to pause the survey and handle other issues before completing the task.

Demographic Makeup of Survey Population

The appendix contains graphical representations of the demographics. The age distribution shows nearly 65 percent of the respondent pool was between 18 and 39 years old. While this is not a perfect representation of the US population, it is expected based on the younger age of the MTurk workforce. Gender results show a 56 percent male majority, which is only a few percentage points higher than the US gender distribution. The distribution of education for the survey respondents shows the vast majority (87.3 percent) had at least some college or technical school education. Income distribution results show about half (48.7 percent) of respondents reported annual household incomes of between $35,000 and $74,999, matching closely with US national income distributions.

The reported political ideology distribution of the respondents shows 53.7 percent of respondents indicated their ideology as left-of-center. Of the remaining respondents, nearly 20 percent identified as being politically neutral, while the remaining 26.6 percent held right-of-center political views. When compared with recent Gallup polling that tracks party affiliation of Americans, the respondent pool is biased left. Gallup generally finds approximately 40 percent of Americans identify as independents, 28 percent as Republican, and 32 percent as Democrats.[180] The different ideological measuring devices between the two surveys and the younger age distribution of the survey experiment population, when compared to a representative population, likely explain the bias.

[180] Gallup. *Party Affiliation Trends Since 2004.* 2019. https://news.gallup.com/poll/15370/party-affiliation.aspx (accessed March 22, 2019).

Some of the demographics are skewed from national averages because the MTurk survey population is not representative of the US population. To validate that the respondent pool still represented a legitimate cross-section of the US population from which to draw scientific conclusions from, respondents were asked, verbatim, a question that Gallup regularly uses in their representative surveys. The question asks respondents to select from a list of 13 events that they worry will happen to them. The list includes cyber attacks, mugging/robberies, car theft, and sexual assault, among others. Results in line with recent Gallup polls would provide evidence that the survey population is a valid representation of the US population, even with some demographics being slightly over or under-sampled. Table 3.1 shows Gallup's October 2018 results along with Gallup's historical average and the results from the survey experiment.[181]

Table 3.1 Survey Experiment Feared Events

How often do you worry about the following things?				
	Gallup Historical Average (%)	Gallup October 2018	Public Survey Respondents	Expert Survey Respondents
Computer Hackers	69	71	56	73
Identity Theft	68	67	48	75
Home burglary when not home	45	40	30	52
Stolen car	43	37	39	27
Your child harmed	32	32	13	33
Getting mugged	29	25	19	13
Victim of terrorism	34	24	19	14
Victim of hate crime	18	22	25	9
Home burglary when home	28	22	9	28
Being attacked while driving	22	22	16	11
Being sexually assaulted	20	20	14	8
Getting murdered	18	17	8	9
Workplace violence	7	7	4	6

[181] Brenan, Megan. "*Cybercrimes Remain Most Worrisome to Americans."* Gallup Polling, November 9, 2018. https://news.gallup.com/poll/15370/party-affiliation.aspx (accessed March 22, 2019).

The intent of this validation question is not to find exact matches in percentages with that of Gallup. Gallup often finds swings in percentages from month to month based on real-world events that have occurred in that particular month (i.e. a large terrorism event would cause worry about terror to spike in the short term). Instead, the intent is to determine if the survey experiment population generally worries about the same things as Gallup's representative population, which the results support. Computer hackers, identity theft, home burglary when not at home, and having a car stolen take the top four spots in all three columns, while workplace violence, murder, sexual assault, being attacked while driving, and home burglary when home take the bottom five spots in all three columns. Overall, the validation question shows a similar pattern in worry between Gallup's representative survey population and the survey experiment's respondent pool. The consistency of responses lends support to the legitimacy of the survey population as a basis for generalizeable scientific findings.

Description of the Expert Survey Population

I recruited the respondents for the expert branch of the survey experiment via individual requests to participate. The 64 experts who participated are government and civilians employees who, by the nature of the work in or with the US government, have above-average knowledge of the cyber domain. While testing for statistical significance is not useful with such a small sample, the results are still significant because they will provide the first-ever survey experiment performed on respondents with a very similar background to the government experts who advise elites and help craft foreign policy.

Demographics data for the experts show, when compared to the public respondents, they are slight older (68.75 percent between the ages of 29 to 49, none younger than 30 years old), mostly male (82.8 percent), and have a higher level of education (95.3 percent postgraduate work

or postgraduate degree). Thirty-eight percent of respondents had ten years or more of experience in the cyber domain, while the remaining had less than 10. As shown above in Table 3.1, the experts also generally worry about the same things as the representative US sample from Gallup polling. Computer hacking, identity theft, and home burglary take the top three spots in both Gallup and the expert populations, while they both match on the least worried items – victim of hate crime, workplace violence, and sexual assault.

Results from the experts that trend in the same direction as the general public pool would provide valuable insight that those in government positions view cyber issues in a similar manner to the general public. If this were the case, then calls for more public input on cyber policy may be less useful then some assume. For example, legal scholar Peter Shane (2012) asserts that leaving the general public out of cyber debates is a "total abdication" of cyber policy to "experts" in the US government and is a "profound mistake" that excludes "the general public from any meaningful voice in cyber policymaking [and] removes citizens from democratic governance in an area where our welfare is deeply implicated."[182] Expert results that skew away from the general public would provide the data needed to support Shane's call for more public input to cyber policy development.

As laid out in the theory in Chapter One, I theorize that I will find no difference in the expert responses for two reasons. First, an analysis of speeches and policy positions from decision-makers shows a strong inclination towards the type of positions I outline in my theory. If having access to additional information on cyber operations nullifies or dampens the theory's causal mechanisms, we should see less expert rhetoric and hyperbole regarding cyber operations and the harm they do or can cause. As shown throughout Chapter one, this is not the case.

[182] Shane, Peter. "Cybersecurity Policy as if "Ordinary Citizens" Mattered: The Case for Public Participation in Cyber Policy Making." *Information Society*. 2012:433-434.

Policymakers appear to have the same high levels of fear and optimism we find from the general public in public polls.

Second, my interactions with cyber professionals and my own experiences lead me to believe that the increase in information that experts have only exacerbates the difficulty in discerning clearly what is happening and what the ramifications are of different operations. I believe this is what has led those with the most amount of insider information, like the former head of US Cyber Command General Alexander, to talk publically about the significant instability the domain causes for decision-makers.

While I hypothesize the experts will trend in the same direction as the public, I believe I may find stronger results for my theory among government cyber experts because of the problems decision-makers face with vast amounts of indiscernible cyber information. The theory would predict that the result of having more information and a better understanding of the strategic instability in the domain would be stronger support for the theory's two main propositions: (1) that experts have an even harder time differentiating between the offense and the defense, and (2) that they have an even stronger belief in the efficacy and need for the offense rather than the defense.

Testing of the First General Proposition

The first theoretical proposition outlined in Chapter One states that people cannot easily distinguish between offensive and defensive cyber activity. This elevates fear levels because citizens and elites cannot easily distinguish the intentions of cyber actors. Strategic instability follows as states struggle to understand and counter cyber activity that does not display clear and discernible intentions. The survey experiment tests six hypotheses that directly relate to this first proposition. The first hypothesis is:

H1: When compared to the modern-day land, air, and sea domains, people believe offensive cyber operations are much more likely to help cyber defense than offensive operations in the other domains are likely to help that given domain (i.e., offensive air operations are not believed to help air defense to the same degree offensive cyber operations can help cyber defenses)

This hypothesis tests how perceptions of the cyber domain differ from the other conflict domains regarding the offense and defense. Support for H1 would lay the foundation for the argument that people view offensive and defensive actions differently in the cyber domain versus other domains. I test this hypothesis by asking survey respondents to select one of four actions that they felt would be most effective at strengthening US defenses in a given domain. The survey randomly assigned participants to one of the four questions, and each question and list of options were identical, with the exception of the domain (e.g., air, land, cyber, and sea). Any statistical difference between responses for the four questions can only be attributed to the domain since all else was identical.

The list of options to strengthen the defense in each domain were (1) use offensive probes in the respective domain to determine enemy capabilities, (2) gather intelligence through traditional sources (e.g. spies, informants), (3) watch and assess enemy actions and exercises, and (4) research and employ new technology in the respective domain. The hypothesis asserts that option one (offensive probe) will receive greater support in the cyber domain than in the other domains. Figure 3.1 shows the results from the question.

Each of the four bars in Figure 3.1 represents the percentage of respondents who chose the offensive probe option as the most effective way to strengthen defenses in the domain they received as part of the randomization process.

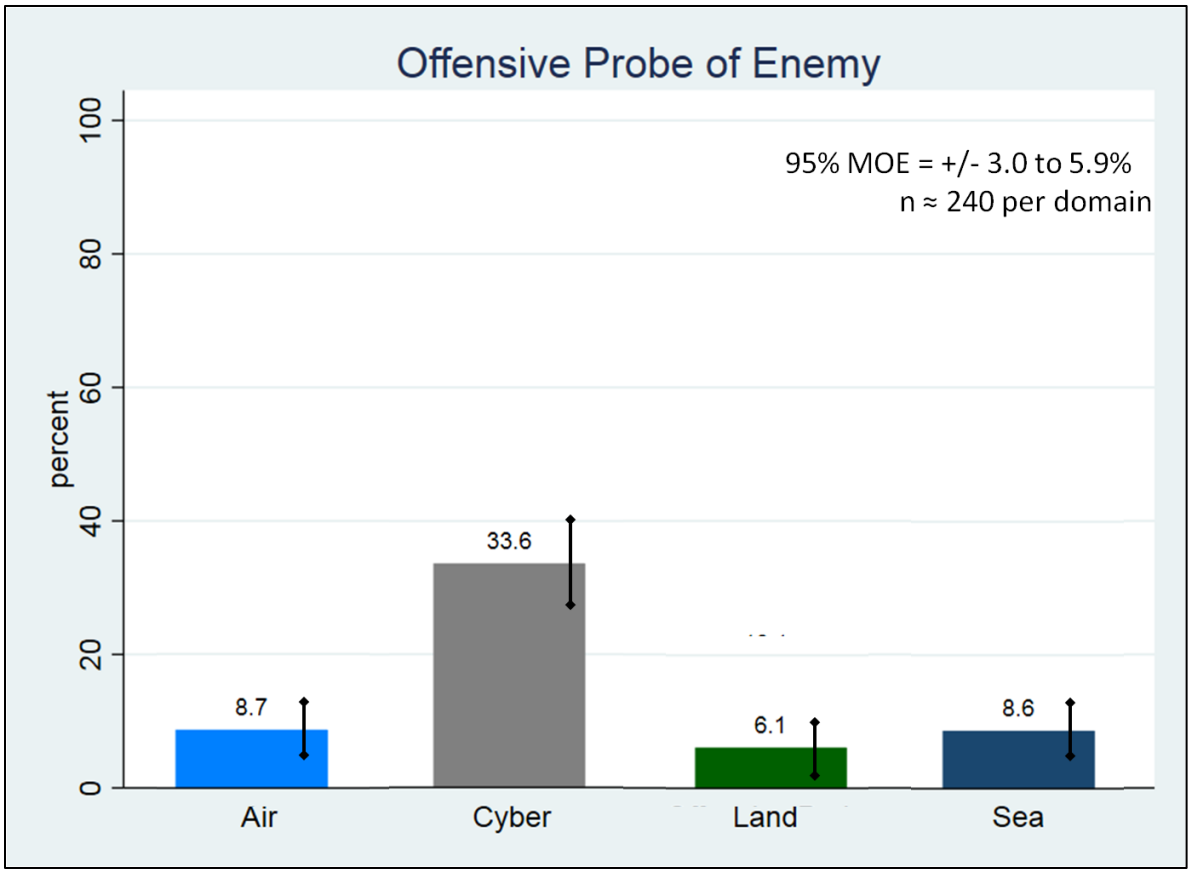


Figure 3.1. Percentage of Respondents Favoring Offensive Probes

Each of the four versions of the question had approximately 240 respondents. The Margins of Error (MOE) were calculated for a 95% confidence level ($z = 1.96$) for each respective bar on the chart. The results show respondents randomized into the cyber domain version of the question chose offensive probes as the most effective way to strengthen cyber defenses at a statistically significant level over respondents randomized into the air, land, and sea domain. Offensive probes as the most effective way to strengthen cyber defenses received 33.6 percent support (5.9 percent MOE), while the air domain received 8.7 percent, ground domain 6.1 percent, and sea domain 8.6 percent (all ≈ 3.0 MOE). In summary, the results support H1. The appendix contains graphs of the support levels for the other three options. The second hypothesis states:

H2: Respondents will give higher support to an offensive probe of an adversary's cyber network if they believe it may yield information that can strengthen US cyber networks against future attacks, versus offensive cyber attacks that yield only general intelligence.

This hypothesis tests the willingness of people to support offensive cyber operations in the name of defensive cyber security. Support for H2 would show that people view offensive cyber actions differently based on whether they believe it will strengthen their cyber defenses. I test this hypothesis by randomizing the respondents into one of two questions. The first question gave a brief description of an offensive cyber probe that the US government wanted to undertake against an adversary. The scenario told respondents that the US government expected the operation to yield intelligence that would help strengthen US cyber defenses. The second question was identical, however, the respondents were told the operation would yield general intelligence for the US government and did not specify that the intelligence would help strengthen US cyber defenses. Respondents had to chose their level of support for the operation on a sliding scale from 0 (no support) to 10 (full support). Table 3.2 shows the results.

The t-test results show that the mean support level for each group is statistically distinct at the p=.05 level (two-tailed) and in the hypothesized direction.

Table 3.2. T-test results for H2.

Group	**Observations**	**Mean**	**S.E.**	**S.D.**	**95% CI**
Gather General Intelligence	466	5.61	.1193	2.57	5.38 – 5.85
Gather Cyber Defense Intelligence	521	6.08	.1110	2.53	5.86 – 6.30
p = .0039 (two tailed), t = -2.89					

The group which was told the offensive cyber operation would produce general intelligence supported the operations with a mean support level of 5.61 and a 95 percent CI of 5.38 to 5.85.

Respondents in the second group, who were told the offensive cyber operation would produce intelligence that could strengthen US cyber defenses, supported the operation with a mean level of 6.08 and a 95 percent CI of 5.86 to 6.30. Figure 3.2 shows the same information in graphical format.

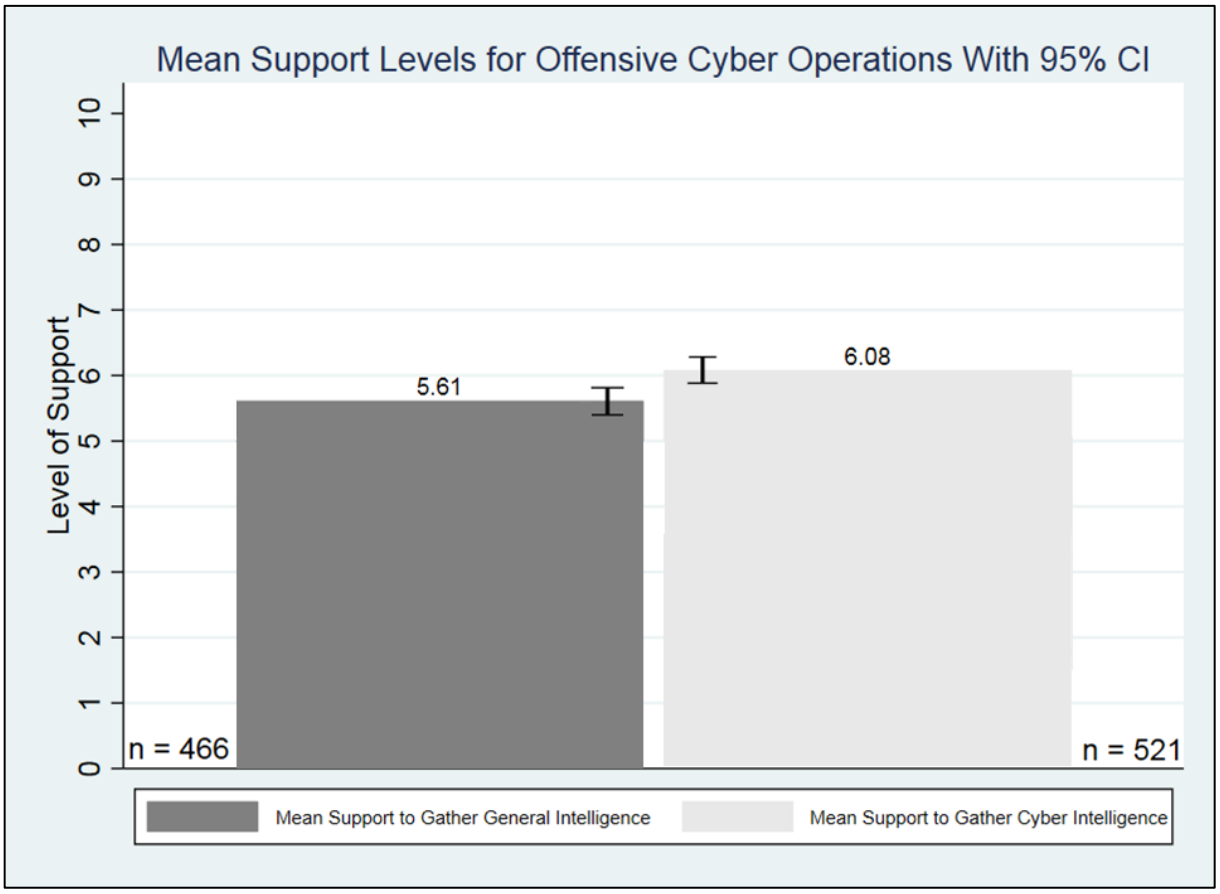


Figure 3.2 Mean Support Levels for Offensive Cyber Operations.

The results support the second hypothesis that people are more willing to support offensive cyber operations if they believe it will help with future cyber defenses versus an offensive cyber operation that produced only general intelligence.

The third hypothesis states:

H3: More people will categorize offensive US cyber operations as 'defensive' if the purpose of the operation is to gather intelligence needed to strengthen US cyber defenses when compared to an identical cyber operation where the objective is to gather generic intelligence.

Positive results for this hypothesis would show that the line between offensive and defensive operations in the cyber domain is easily obfuscated based on stated mission objectives. The blurring of this line helps create the strategic instability seen in the cyber domain as states undertake multiple offensive operations but often couch their support for such operations in defensive terms. The survey experiment tests this hypothesis by randomizing respondents into one of two groups. The first group received a scenario that said the US often undertakes cyber operations against adversaries, and that the goal of these operations was to gather general intelligence. Respondents were then asked to classify the US operation as either offensive or defensive in nature. The second group was given an identical scenario, except the goal of the operation was to gather intelligence needed to increase US cybersecurity. The theory presented in Chapter One asserts that more people in the second group will classify the operation as defensive versus the first group simply because the stated objective is different for an otherwise identical cyber operation. Figure 3.3 (next page) shows the results from the group told that the cyber operation was designed to gather general intelligence.

The results show 60.59 percent of respondents classified the mission as offensive, while the remaining 39.41 percent classified it as defensive. The 95 percent confidence MOE is +/- 6.2 percent, with no overlap between responses. To thoroughly test H3, these results must be compared against the findings from the second group of respondents who were told the objectives of the operation were to gather intelligence for cybersecurity.

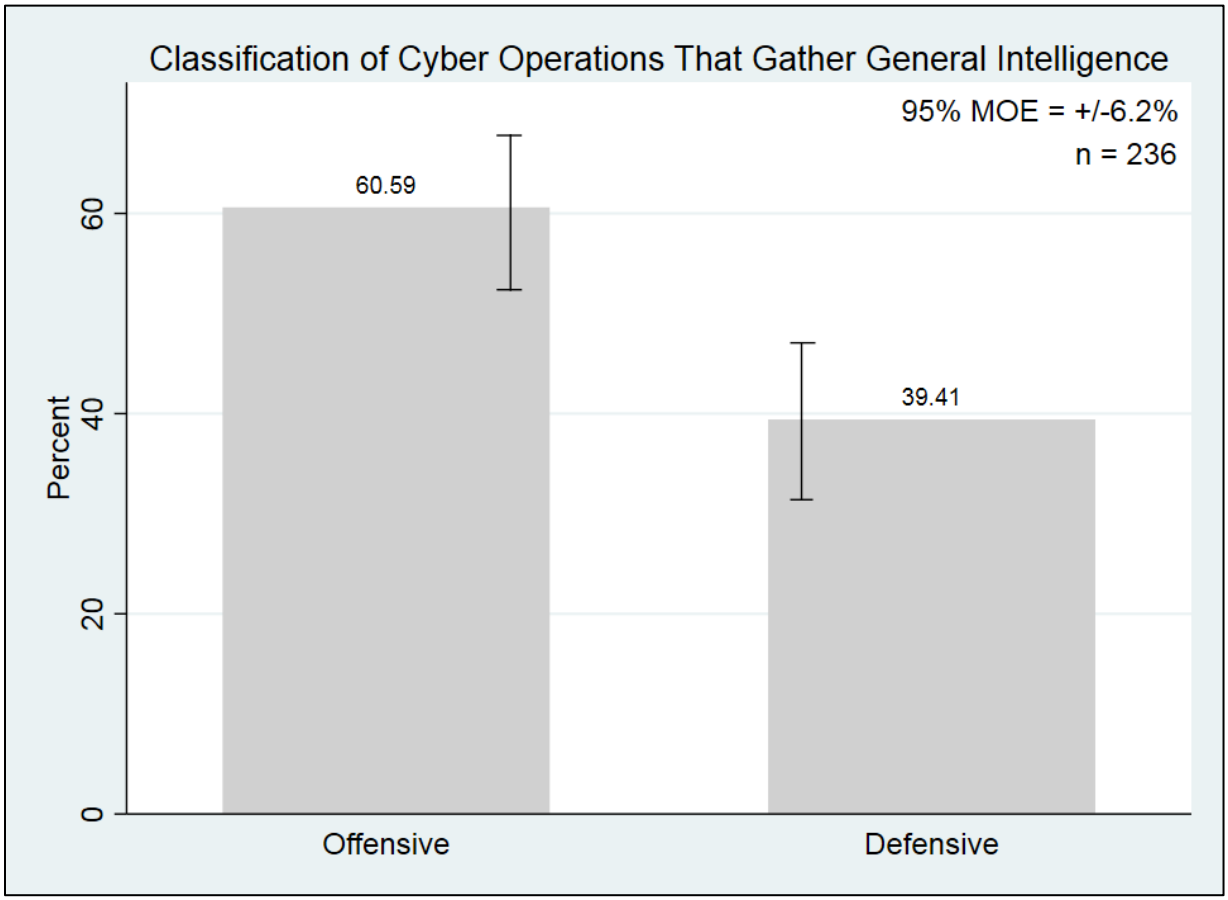


Figure 3.3 Classification of Cyber Operations Gathering General Intelligence.

Figure 3.4 (next page) shows the results from the second group. As the graphic shows, there was nearly a complete reversal in responses after the treatment. The results show 61.29 percent of respondents, when told the objective of the cyber operation was to gather intelligence for cybersecurity, changed the classification of the mission to defensive, while the remaining 38.71 percent classified it as offensive. This represents a near mirror image of the results from the first group, where the objective of an identical cyber operation was to collect general intelligence for the US government.

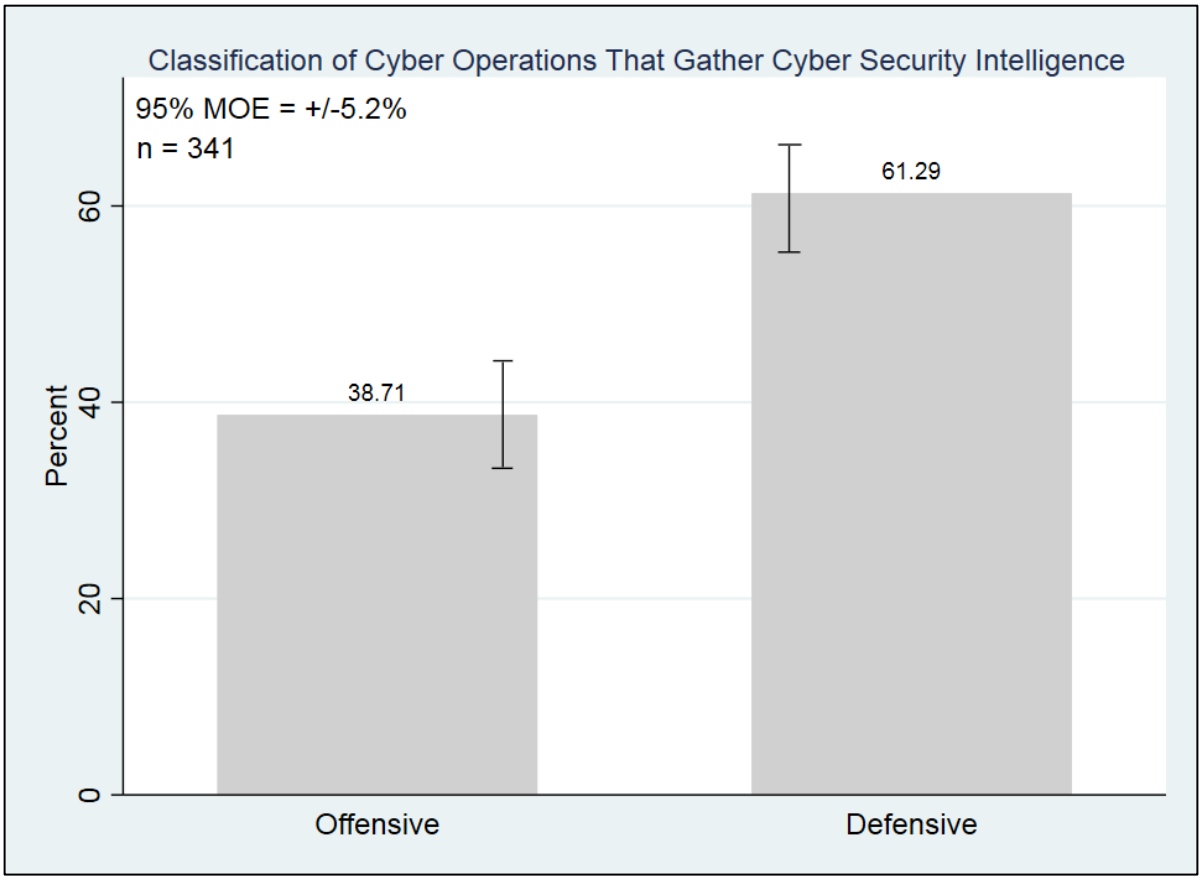


Figure 3.4 Classifications of Cyber Operations Gathering Cyber Security Intelligence.

The results show that the treatment (telling respondents the cyber operation was going to collect cybersecurity intelligence versus general intelligence) caused the number of respondents who classified the mission as defensive to increase from 39.41 percent in the first group to 61.29 percent in the second group. The change equates to a 21.88 percent increase, which is a statistically significant finding given the 95 percent confidence MOEs of 6.2 percent and 5.2 percent between the two groups. In sum, the findings support H3 and lend support to the theoretical proposition that people alter their opinion of what is offensive versus what is defensive based only on stated mission objectives for otherwise identical cyber operations.

Hypothesis four is directly related to H3. It states:

H4: When presented with a scenario where an adversary undertakes offensive cyber operations against the US, people will generally classify this as an offensive operation, even when told the adversary undertook the operation to strengthen their own cyber defenses.

This hypothesis is essentially H3 but from the adversary's perspective. Positive results would support the theoretical tenet that cyber operations nearly always look offensive to the attacked state, even if the state doing the attacking does not believe their operations are offensive (e.g. H3). Testing this hypothesis entailed a nearly identical approach as that used for H3. Respondents were given the same scenario from H3; however, the scenario said the cyber operation was being undertaken against the US by an adversary state. The first scenario told the group of respondents that the other state undertook the action to collect general intelligence for their government, while the second scenario told participants that the operation was used to collect intelligence needed for cybersecurity for the state who undertook the operation. To add validity to the results, none of the respondents randomized into the H3 scenario also received the H4 scenario and vice versa. Figure 3.5 (next page) shows the results from the first group.

The results show 78.23 percent of respondents classified adversary cyber operations designed to gather general intelligence as offensive, while the remaining 21.77 percent believed it to be defensive. The 95 percent MOE is +/- 5.1 percent with an n of 248. When compared to the same scenario in H3, except where the US was the nation undertaking the cyber operation, this represents a 17.64 percent increase in those who felt the action is offensive. Given the MOEs for each survey, this increase is statistically significant and shows that simply altering the state that undertakes an otherwise identical cyber operation causes significant shifts in perceptions of offense versus defense.

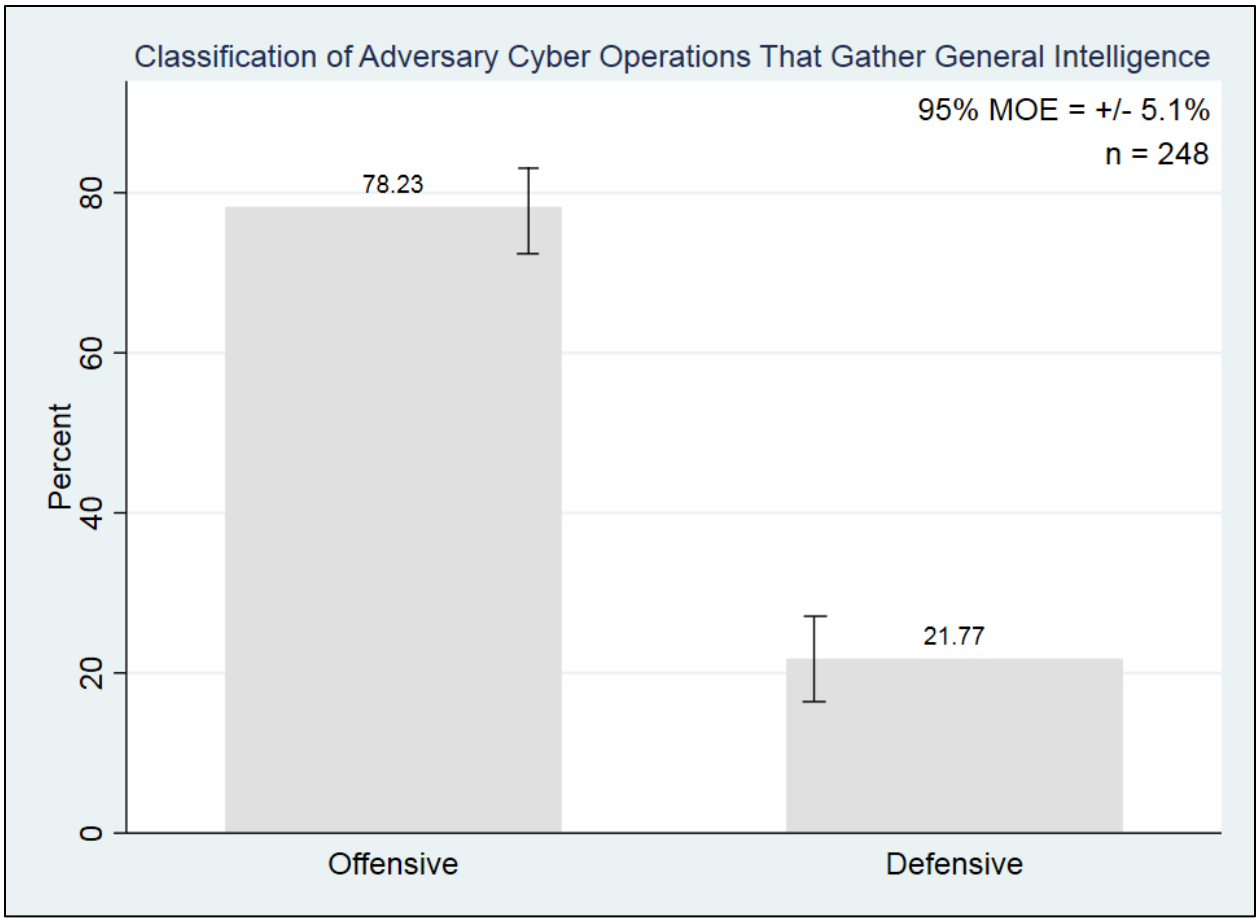


Figure 3.5 Classification of Enemy Cyber Operations for General Intelligence.

The second group of respondents for H4 received the same scenario as the first, except the objective of the adversary nation undertaking the cyber operation was to gather intelligence to bolder their cyber-security. Figure 3.6 (next page) shows the results.

Contrary to the theory, the results show that people still shifted their perceptions of whether the attack was offensive or defensive even when the scenario is about another state conducting operations against the US. The difference between those who considered it offensive versus defensive is 12.16 percent. With a 6 percent MOE, any difference greater than 12 percent meets the criteria for statistical significance. These results leave H4 as being only partially supported.

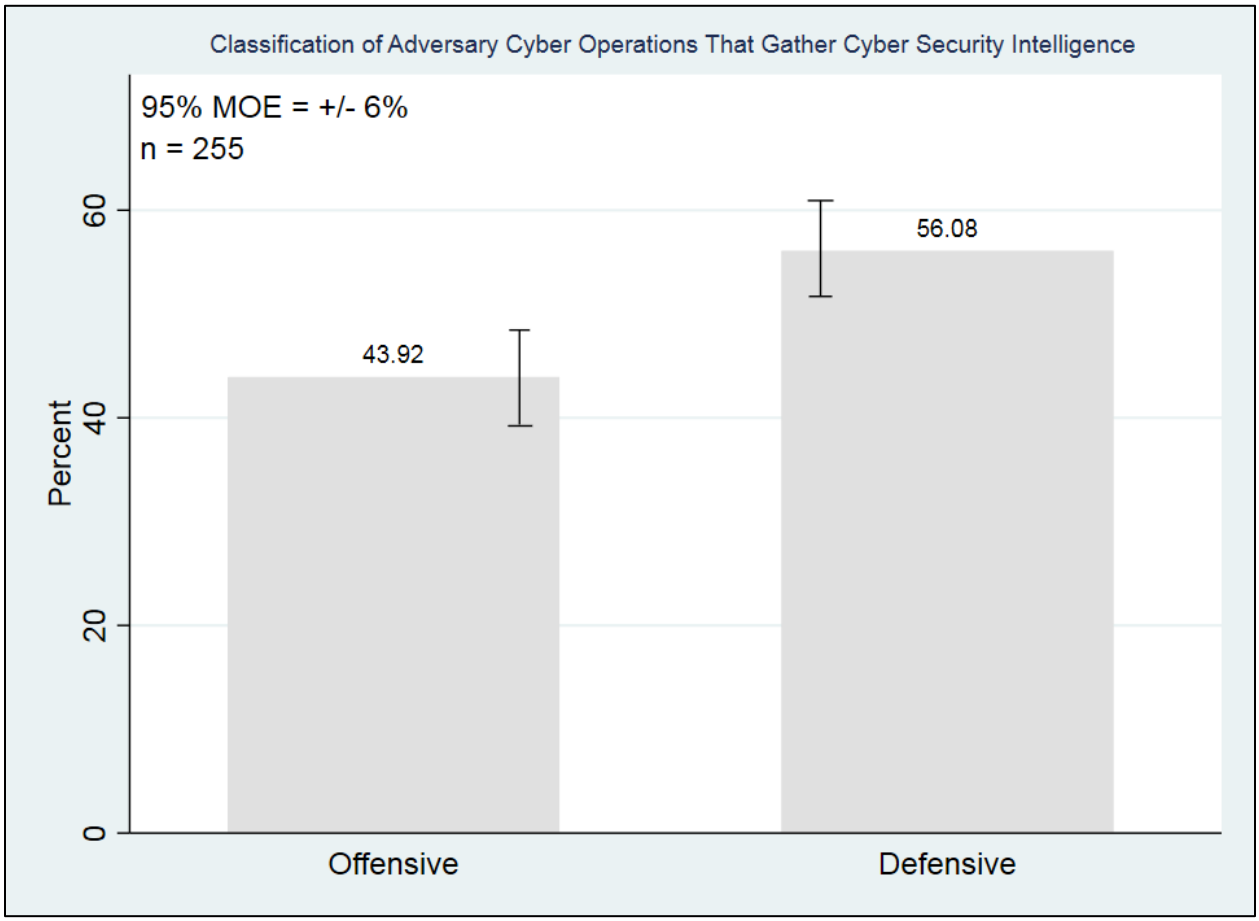


Figure 3.6 Classification of Enemy Cyber Operations for Cyber Security Intelligence.

Nearly 80 percent of respondents said adversary cyber operations conducted against the US to collect general intelligence were offensive, and this rate exceeded the H3 scenario by nearly 20 points (outside the 95 percent MOE). The results show that respondents were more willing to classify a cyber operation as offensive when another state undertook it, versus when the US undertook an identical operation, which lends support to H4. However, the second group of respondents still flipped the offense/defense response rates when told that the adversary's operation was designed to collect cybersecurity intelligence. The shift was not as significant as it was for the US scenario in H3, however, the shift met significance standards and was not predicted by the theory, leaving H4 with only partial support.

Testing of the Second General Proposition

The second general proposition outlined in the theory presented in Chapter One is that people view national cyber defense as the status quo and not as an exploitable concept that can offer measurable gains when compared to offensive operations. Simply put, the theory proposes that the offense has the advantage in the cyber domain. The predicted result is that people will want to continually exploit the offense for gains, even if the data show negligible gains from such operations. There are three hypotheses within the survey experiment to test this proposition.

The first is H5, which states:

H5: People believe that higher levels of offensive cyber capabilities are more advantageous than higher levels of cyber defense.

I test this hypothesis in the survey experiment by asking all respondents to select a national cyber strategy that they believe would be most beneficial for the US over the next decade. The first strategy (Strategy A in the survey experiment – the offensive strategy) focused on cyber capabilities that could penetrate enemy networks, fight and disrupt enemies without the need for traditional US military forces (e.g. ground soldiers, airplanes, etc), and gather nearly any intelligence US leaders needed to protected US residents and economic interests.

The second strategy (Strategy B in the survey experiment – the defensive strategy) focused on capabilities that could detect nearly any enemy cyber-attack, better protect US military forces from disruptive enemy cyber attacks, and better protect US networks against cyber attacks that could provide intelligence to enemy leaders. Figure 3.7 (next page) gives a graphical representation of the results.

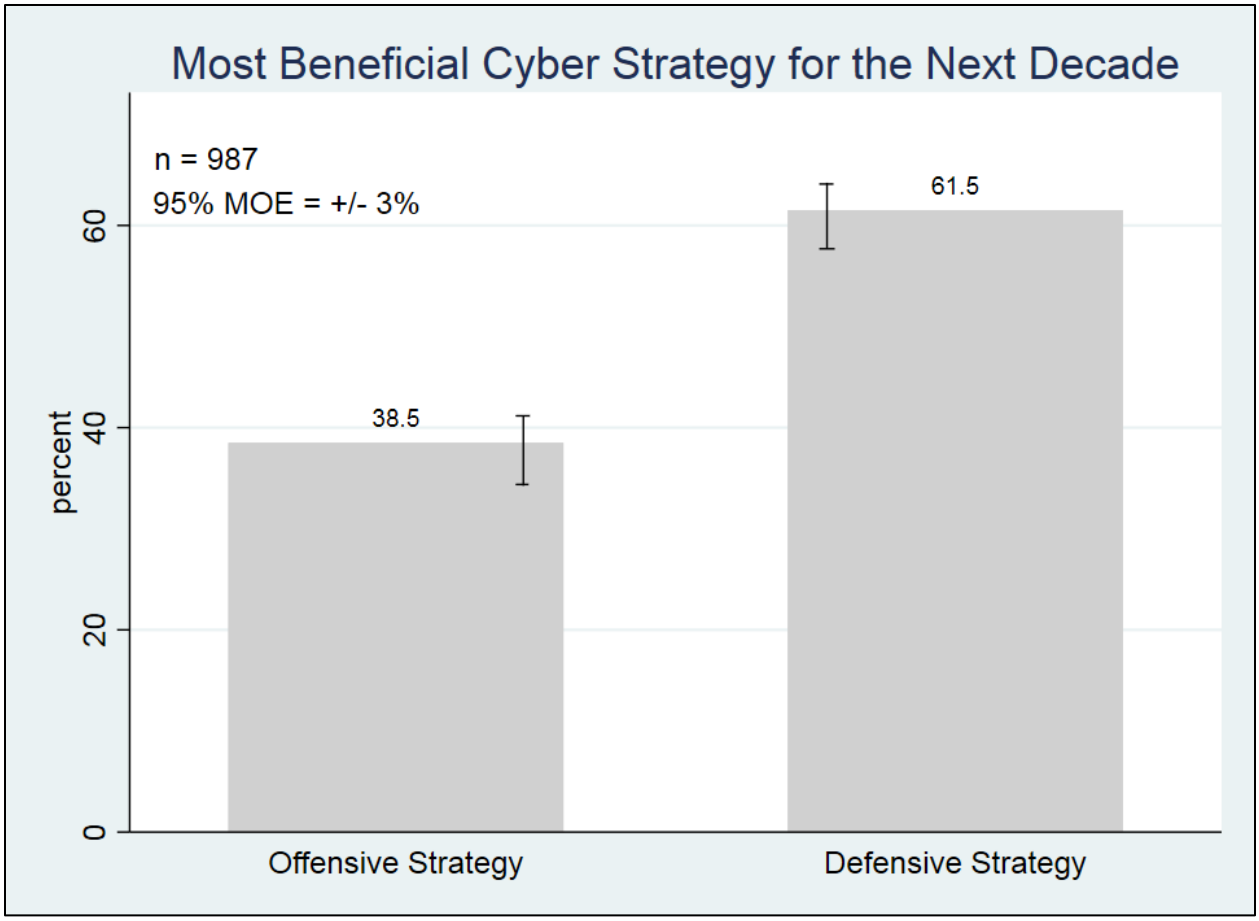


Figure 3.7 Most Beneficial US Cyber Strategy for the Next Decade.

The data show that H5 is unsupported. Sixty-one and a half percent of respondents chose the defensive strategy as the best option for the US to pursue for the next decade versus 38.5 percent of respondents who chose the offensive strategy. With a 95 percent MOE of +/- 3 percent, the results are statistically distinct. The displayed policy preference may stem from the fact that cyber attacks are the most feared crime among Americans, as discussed in Chapter One, and thus respondents may have opted for the defensive strategy in hopes it would quell their fear. Another factor that may have caused this unpredicted response is the fact that America's offensive cyber capabilities are robust and well-known after various leaks detailing the inner workings of US government cyber operations. With this information, respondents may have felt

that US offensive cyber capabilities were already in place, and thus they preferred a focus on more robust cyber defenses.

The next hypothesis states:

H6: Adversaries who spend more money on cyber defense then cyber offense are less threatening to respondents.

This hypothesis stems from the theory's prediction that people view cyber defense as intrinsic and required for the domain. Thus, an adversary who spends money on cyber defenses in less threatening than one who spends money on offensive cyber capabilities. The survey experiment tests this hypothesis by presenting respondents with three notional adversaries who were all identical except in their budgets for the cyber domain. I then asked respondents to select which nation was the least threatening. Nation A's budget apportioned $1 billion for cyber offense and $9 billion for cyber defense, while Nation B spent $9 billion on offense and $1 billion on defense, and lastly, Nation C spend $5 billion on each. The results are graphed in Figure 3.8 (next page).

The overwhelming majority of respondents felt Nation A, which dedicated 90 percent of its cyber budget to defensive capabilities and only 10 percent to offensive ones, was the least threatening nation to US interests. These results reinforce the theory's prediction that the efficacy of cyber offense creates fear among respondents far more than cyber defenses do. As discussed in Chapter One, the ease at which a state can penetrate another state's cyber networks, and take nearly anything, underlies this finding. The findings lend support to the second general proposition.

The last hypothesis states:

H7: People do not believe strengthening cyber defenses is an effective strategy against antagonistic cyber activity or against adversaries in general.

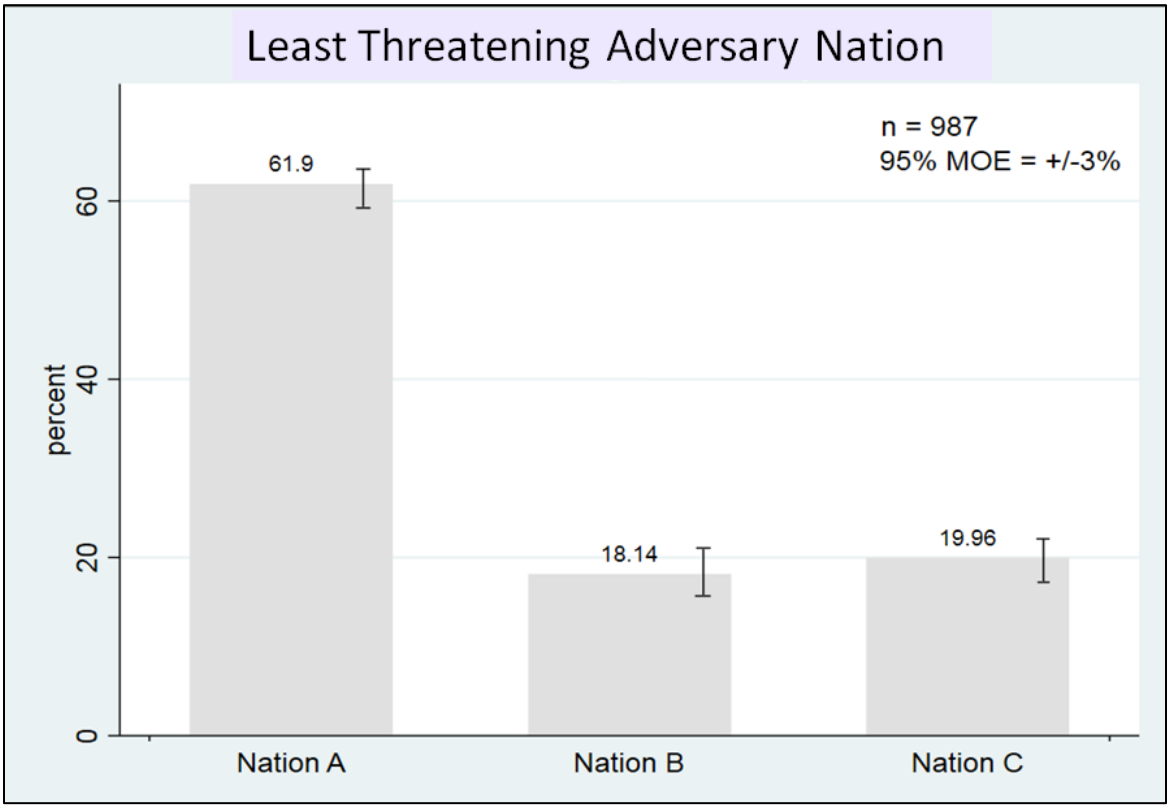


Figure 3.8. Percent of Respondents who Viewed Each Nation as Least Threatening.

The theory postulates that people believe in the efficacy of the offense over that of the defense. Thus, when faced with adversarial cyber activity, respondents will opt for strategies that rely on offensive capabilities rather than defensive ones. This stems from the assertion that adequate cyber defenses rarely (if ever) exist as it seems those who are intent on breaking into a network will do it one way or another. Thus, the theory predicts respondents will prefer an offensive strategy to combat nefarious cyber activity, just as elites have chosen to do for the past three decades as detailed in Chapters One and Two. The survey presented respondents with a scenario where US officials needed to decide how to allocate $10 billion for future US cyber capabilities. Respondents had to select what mixture of offense versus defense they wished the

government spent the money on. Selecting zero meant allocating all of the money towards defensive capabilities, while five represented a 50/50 split, and ten represented investing only in offensive capabilities. Respondents could select any number between 0 and 10. Figure 3.9 shows the percentage of respondents who selected each given number on the sliding scale.

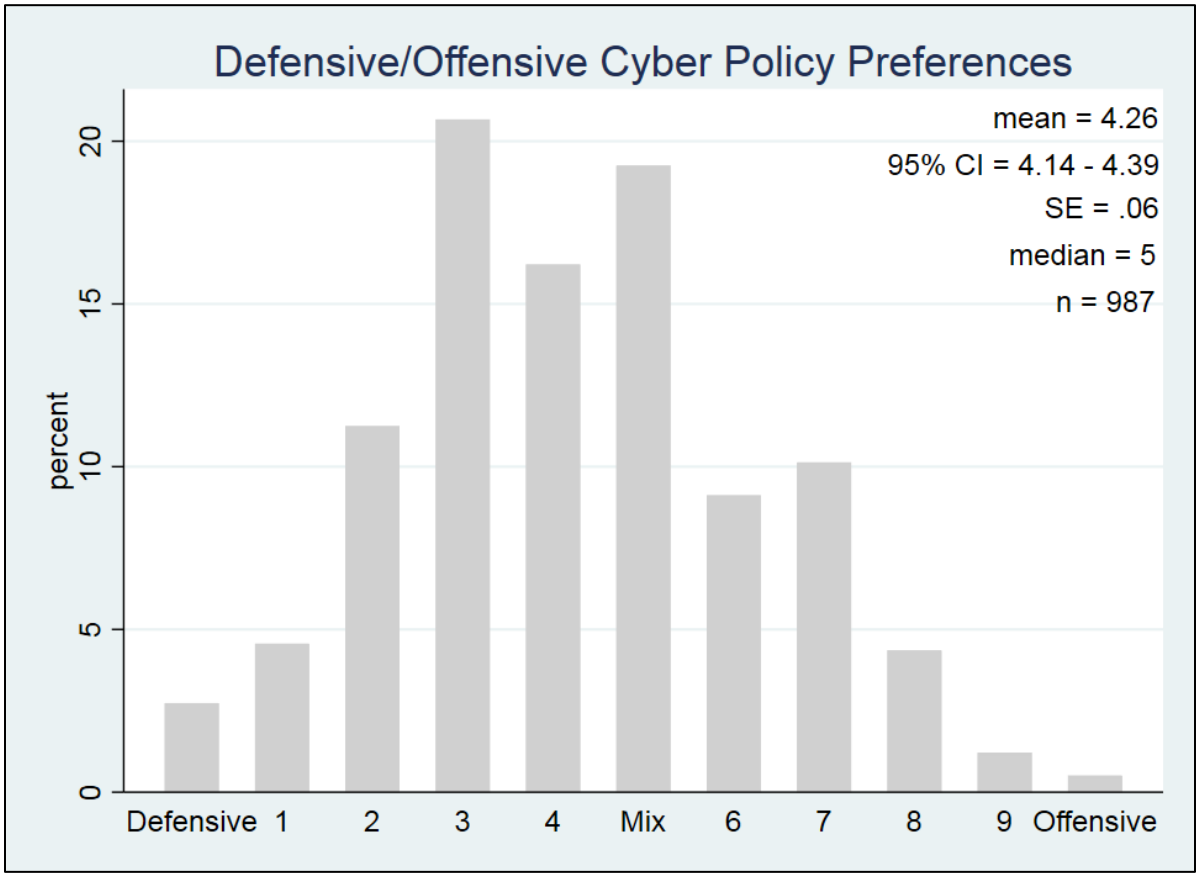


Figure 3.9 Sliding Scale Response Percentages for Offensive vs Defensive Budget Allocation

The results show that the 987 respondents preferred a more defensive allocation of the money as the mean sliding scale value is 4.26, with a 95 percent CI of 4.14 to 4.39. With 5 representing a 50/50 mix of offense and defense, any mean less than 5 is a defensive allocation of the money. Of the 987 respondents, 547 (55.42 percent) selected a value between zero and four, indicating a desire for a more defensive allocation. One hundred and ninety (19.25 percent) chose a 50/50 mix value of five, while the remaining 250 respondents (25.33 percent) opted for

an offensive allocation of money by selecting a value between six and 10. In short, this hypothesis is not supported as the results show a desire for a more defensive allocation of the notional cyber budget.

Discussion of Results

The first general proposition posited in Chapter one stated that the offense and defense are difficult to distinguish in the cyber domain. Hypotheses 1-4 were designed to test this proposition in several different ways. The results from testing each hypothesis support this general proposition. Testing for H1 showed that a statistically distinct percentage of respondents felt offensively probing the enemy was the most effective means of strengthening cyber defenses when compared to offensive probes in the sea, land, and air domain. These results lend support to the theoretical argument that there is a perception that strong cyber defenses rely on offensive cyber operations at a much higher rate than offensive operations in any of the other three domains would help defenses in that given domain.

Hypothesis two stated that people would support an offensive cyber operation that gathered intelligence needed to strengthen cybersecurity at a higher rate than they would for a cyber operation designed to collect only general intelligence. The results show a higher and statistically distinct level of support for such operations, which lends support to the argument that offensive cyber operations are part of an effective defensive cyber strategy. In turn, this supports the position that the defense and offense are hard to distinguish in the cyber domain.

Hypothesis three asserted that people would classify a cyber operation as 'offensive' or 'defensive' differently based on what the stated objective of the cyber intrusion was. The results show 61.29 percent of respondents who were told the objective of a cyber operation was to gather intelligence for cybersecurity classified the mission as defensive, while the remaining

38.71 percent classified it as offensive. When contrasted with the first group, the results are a near mirror image from the group who believed the objective of the cyber operation was to collect general intelligence for the US government.

The treatment (telling respondents the cyber operation was designed to collect cybersecurity intelligence versus general intelligence) caused the number of respondents who classified the mission as defensive to increase from 39.41 percent in the first group to 61.29 percent in the second group. The 21.88 percent increase is statistically distinct and offers further evidence that the line between the offense and the defense is easily obfuscated and difficult to distinguish.

The last hypothesis, H4, stated that people would be more apt to label an adversary's cyber operation as offensive, even when told the adversary was undertaking the operation to gather cybersecurity intelligence. Contrary to the theory, people still shifted their classification of the operation just as they did in H3. While this is the opposite of what the theory predicted, it does little to undermine the theory's foundation. The reason for this is because when an adversary undertakes a cyber operation, they will never advertise their objectives before, or during the cyber attack. In the scenario for H4, the respondents were given this information because it was needed to test the hypothesis. In short, while the results for H4 were opposite from the prediction, it is difficult to apply this to the real world because the amount of information given in H4 is not realistic. It was designed to test a specific aspect of the theory. The theory, however, still gains strong support even in light of the null findings for H4. In summary, the data collected from the four hypotheses offers support for the first general proposition that the defense and offense are challenging to distinguish in the cyber domain.

Results designed to test the second general proposition show less support for the hypotheses then the theory predicts. The second general proposition supposes that people view national cyber defense as the status quo and not as an exploitable concept that can offer measurable gains when compared to offensive operations. Simply put, the theory proposes that the offense has the advantage in the cyber domain, and it means that people will want to continually exploit the offense for gains, even if the data show negligible gains from such operations. There are three hypotheses within the survey experiment to test this proposition.

Hypothesis five asked respondents to choose between two cyber strategies that they felt would be most effective over the next decade. The first strategy was offensively-oriented, while the second strategy was defensive. The results show 38.5 percent of respondents chose the offensive strategy, while 61.5 percent of respondents chose the defensive strategy, which is a null finding for H5. There several reasons respondents may have contradicted the theory. First, US offensive cyber capabilities are well-known after many widely-advertised leaks of US cyber programs (e.g. Snowden leaks). Respondents may have felt comfortable with the United State's offensive capabilities in the cyber domain and may have wanted to focus on better network protection. Second, since cyber attacks are the most feared type of crime, as shown in Chapter One, respondents may have opted for a defensive strategy to quell their fears about cyber attacks; even despite the fact data show cyber attacks are not measurably impacting Americans. In either case, the results do not support the second proposition.

Hypothesis six asked respondents to assess which of the three countries was the most threatening to the US. The states were identical except in their cyber budgets. Nation A's budget included $1 billion on cyber offense and $9 billion on cyber defense, while Nation B spent $9 billion on offense and $1 billion on defense, and lastly, Nation C spend $5 billion on

each. This hypothesis stems from the theory's prediction that people view cyber defense as intrinsic and required for the domain. Thus, an adversary who spends money on cyber defenses in less threatening than one who spends money on offensive cyber capabilities. The results showed that respondents overwhelmingly chose the state that spent 90 percent of its budget on offensive cyber capabilities as the most threatening state.

While this may seem like a common-sense finding, because one of the three states spends a disproportionate of their budget on offensive cyber capabilities, it is essential to note that the historical record shows offensive cyber weapons have caused little-to-no damage to a state, and have not been shown to alter the political calculus of a state. Strong cyber defenses, however, have shown the ability to cause angst among political elites. For example, North Korea, often a source of agitation among Washington political leaders, has strong cyber defenses. Offensive cyber probes designed to gather intelligence and help elites understand the intentions of a state like North Korea are far less effective than they would be otherwise.

When the intentions of another state cannot be discerned, either through open dialogue or through intelligence gathering methods, it creates political instability that can make conflict more likely. In short, it is not unlikely that an adversary be more threatening with strong cyber defenses because it may allow them to develop other weapons and undertake operations without the fear of network penetrations revealing their secrets and intentions. As the theory predicted, however, respondents felt the state that spent most of its money on offensive cyber capabilities was the most threatening. Thus, despite limited data to support the notion that offensive cyber operations can measurably help states, respondents still believe in the efficacy of the offensive, which supports the second proposition.

Hypothesis six was the final test of the second proposition. This hypothesis asked respondents to select the offensive/defensive ratio they preferred for US cyber budgets by moving a sliding scale from 0 to 10. Zero was fully defensive, while ten was fully offensive. The results show that the 987 respondents preferred a more defensive allocation of the money as the mean sliding scale value is 4.26 with a 95 percent CI of 4.14 to 4.39. With 5 representing a 50/50 mix of offense and defense, the mean 4.26 value shows a slight skew towards a defensive allocation of the budget and is a null finding for H6. As with the null findings for H4, respondents may have opted for a budget allocation with a slight defensive skew because of their fear of cyber weapons, or because of their perception that offensive US cyber forces are already adequately funded. As a result, the second general proposition ends up only partially supported by the survey experiment respondents.

Cyber Expert Respondents

I conducted an additional round of the survey experiment on a small group of people who had above-average knowledge of the cyber domain. The purpose of this experiment is to determine if having more knowledge of the cyber domain will elicit different responses to the questions. The 64 experts recruited for this round of the experiment had either US military experience or are civilian scholars who work with the US military daily. Some of the respondents were true experts in the cyber field, holding positions within the US military cyber corps. Other respondents were academics or military members who did not work directly in the cyber field, but by the nature of their work in and around the US military, had exposure to discussions and briefings that gave them additional knowledge of the cyber domain that respondents in the original experiment would not likely have.

Because the pool of respondents is small, there is no ability to conduct statistical significance tests. Significance tests become even more problematic as several of the scenarios randomized respondents into as many as four categories. Instead, the purpose of this smaller survey is to see if these experts generally trend in the same direction as the broader US respondent pool. Conducting the survey experiment on a larger pool of cyber experts would be a useful future research project for further theory testing.

The first question randomized the respondents into one of four scenarios representing the four military operational domains – air, cyber, land, and sea. Each respondent had to pick one out of four answers that they felt would be most beneficial to strengthening the given domain. The options were probing the adversary, gathering intelligence through traditional means (e.g., spies, informants), watching and assessing the enemy to determine capabilities, and researching and employing new technology. Figure 3.10 shows the expert responses (red diamonds) overlaid on the original survey results.

The expert results mirror the general survey experiment respondent results. Overall, the experts felt probing adversary cyber networks was the most effective strategy to strengthen US cyber defenses at a rate much higher than probing would help in the other three domains. As previously mentioned, no statistical significant tests are useful based on the n of each group (cyber = 11, air = 12, sea = 23, and land = 19). However, the results do show that the experts trended in the same direction as the general public in their desired response.

The next test randomized the experts into two different scenarios to test H2. The first scenario asked for their general level of support, from 0 (no support) to 10 (full support) for a cyber operation that would produce general intelligence.

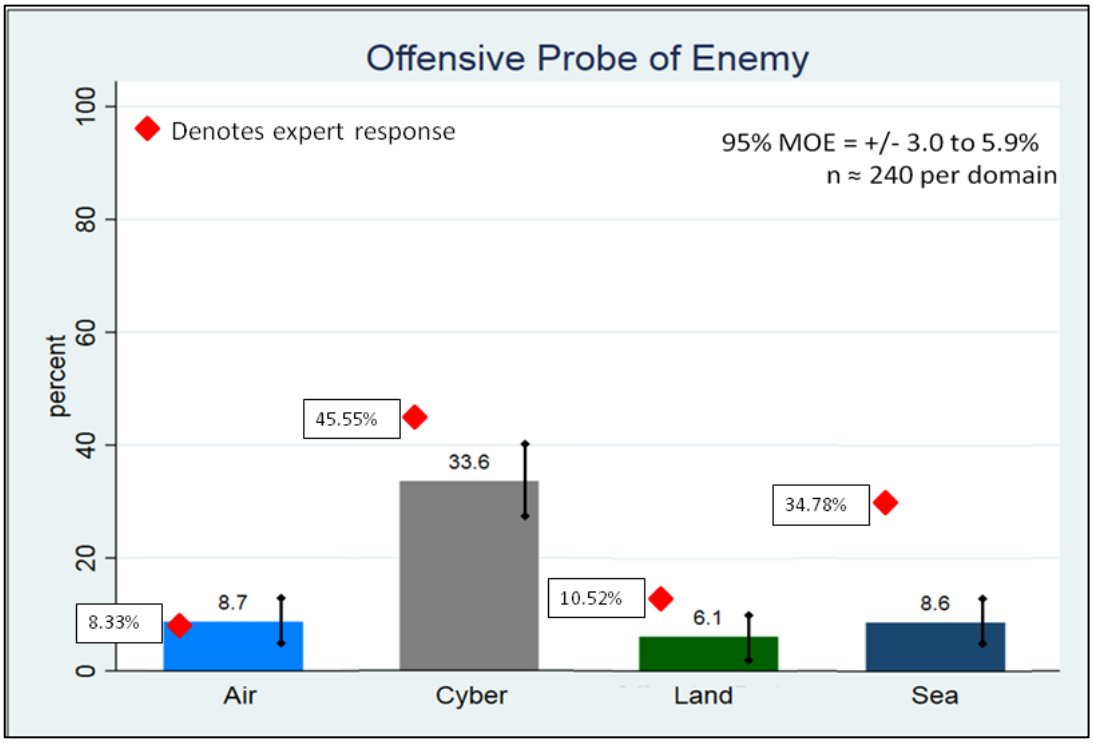


Figure 3.10 H1 Expert Responses

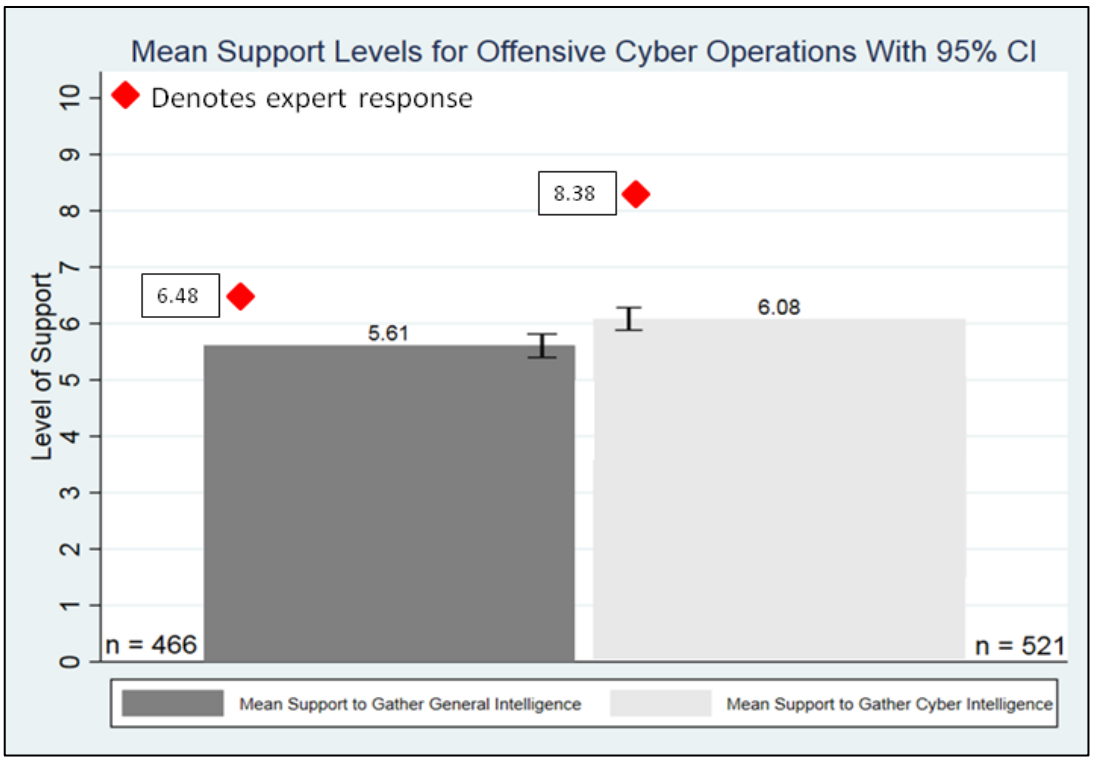


Figure 3.11 H2 Expert Responses

Those randomized into the second scenario had to indicate their level of support for a cyber mission that would produce intelligence needed to better secure US cyber networks. Figure 3.11 shows the expert responses overlaid on the original graph for H2.

The next question randomized the experts into two groups to test H3. The first group had to classify a cyber operation designed to gather general intelligence as either offensive or defensive. Figure 3.12 shows the expert results.

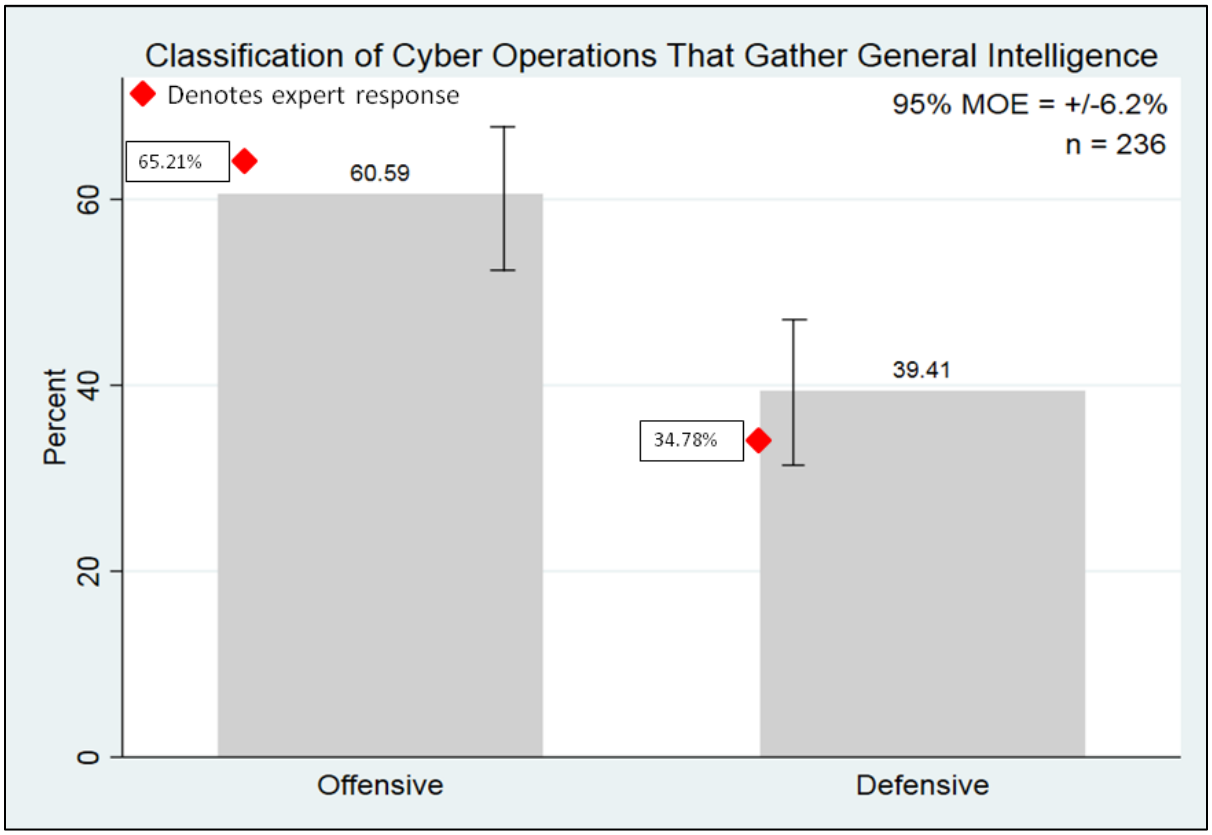


Figure 3.12 H3.1 Expert Responses

Again, we find the experts mirrored the general population in their responses, as 65.21 percent of experts classified a cyber operation designed to gather general intelligence as offensive, while the remaining 34.78 percent of experts classified it as defensive. The second group of experts received a scenario identical to the previous except they were told the operation

would produce intelligence that would strengthen US cyber defenses. Figure 3.13 shows the expert responses overlaid on the original graph.

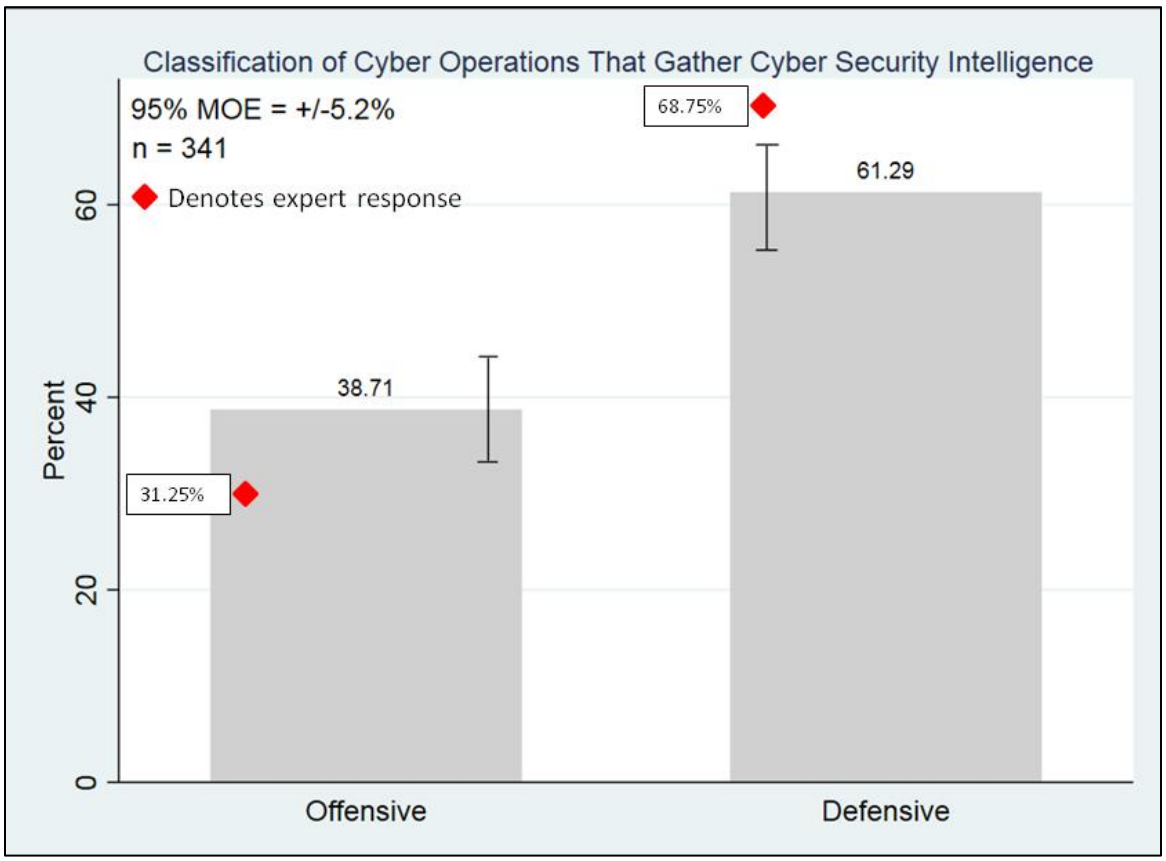


Figure 3.13 H3.2 Expert Responses.

Again, we find the experts mirror the general population, as 31.25 percent classified a cyber operation designed to gather intelligence that can strengthen US defenses as offensive, while 68.75 percent classify it as defensive. As with the general public, the experts flipped the classification of the mission simply because the stated objectives of the cyber mission changed. As discussed earlier, this presents a problem for military and political leaders. It shows that people are willing to undertake a cyber mission to gain intelligence to bolster cyber defenses, and they rationalize the mission as defensive. The problem occurs for the attacked state because they cannot discern whether a cyber attack is just an intelligence-gathering mission or a more

nefarious cyber attack designed to plant logic bombs, corrupt networks, or many other more damaging scenarios. Thus, the attacked state must assume the worst-case scenario, while the state undertaking the attack sees the mission as a defensive mission.

The next question tests H4 by asking respondents to classify an adversary's cyber attack as either offensive or defense. One group of respondents received a scenario where the objective of the adversary's attack was to gather general intelligence. The second group's scenario said the objective of the adversary's cyber attack was to gather the intelligence needed to strengthen the adversary's cyber defenses. These two scenarios are essentially the scenarios from the previous hypothesis, except from the adversary's perspective. Figure 3.14 graphs the results collected from the first group.

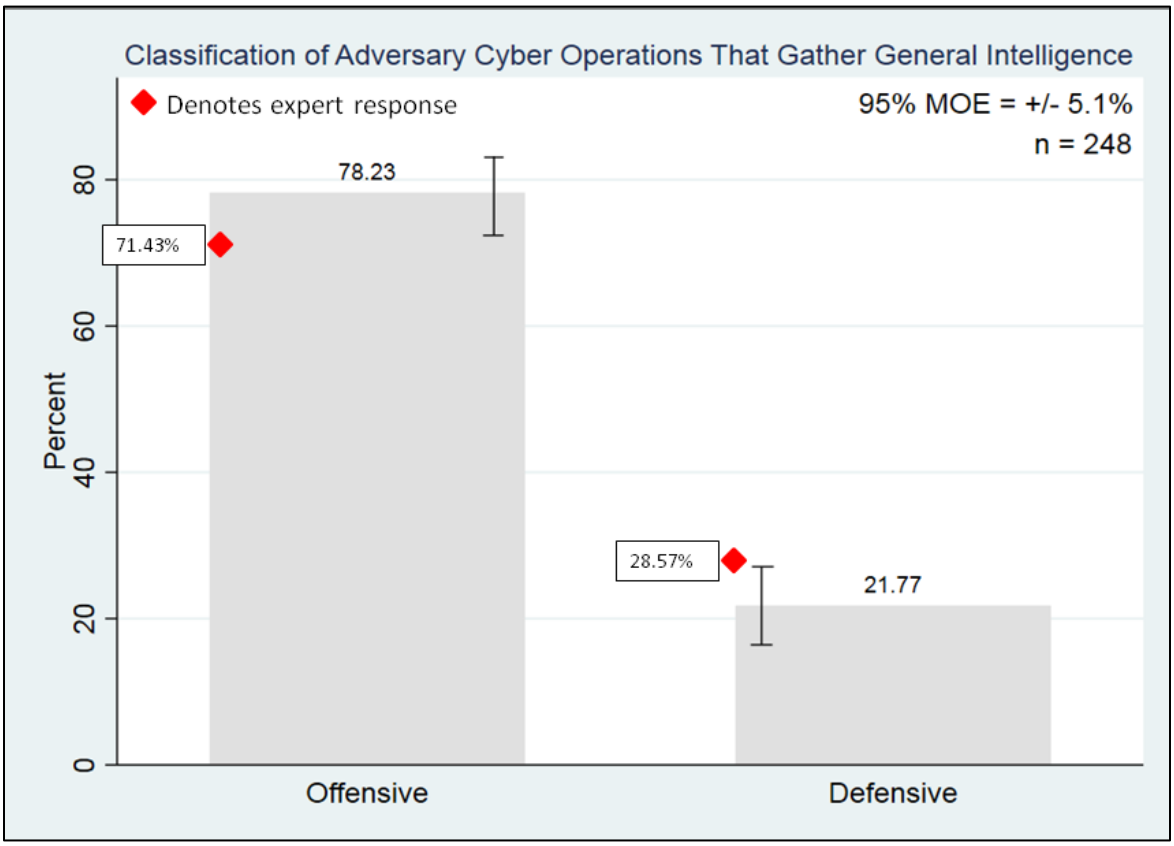


Figure 3.14 H4.1 Expert Responses.

As with the previous hypotheses, the expert responses mirrored those of the general public. The majority of experts classified the enemy cyber attack that was designed to gather general intelligence as offensive in nature. The next group of experts received the same scenario, except the objective of the adversary's cyber attack was to gather intelligence needed to strengthen the enemy's cyber networks. Figure 3.15 gives a graphical representation of the results.

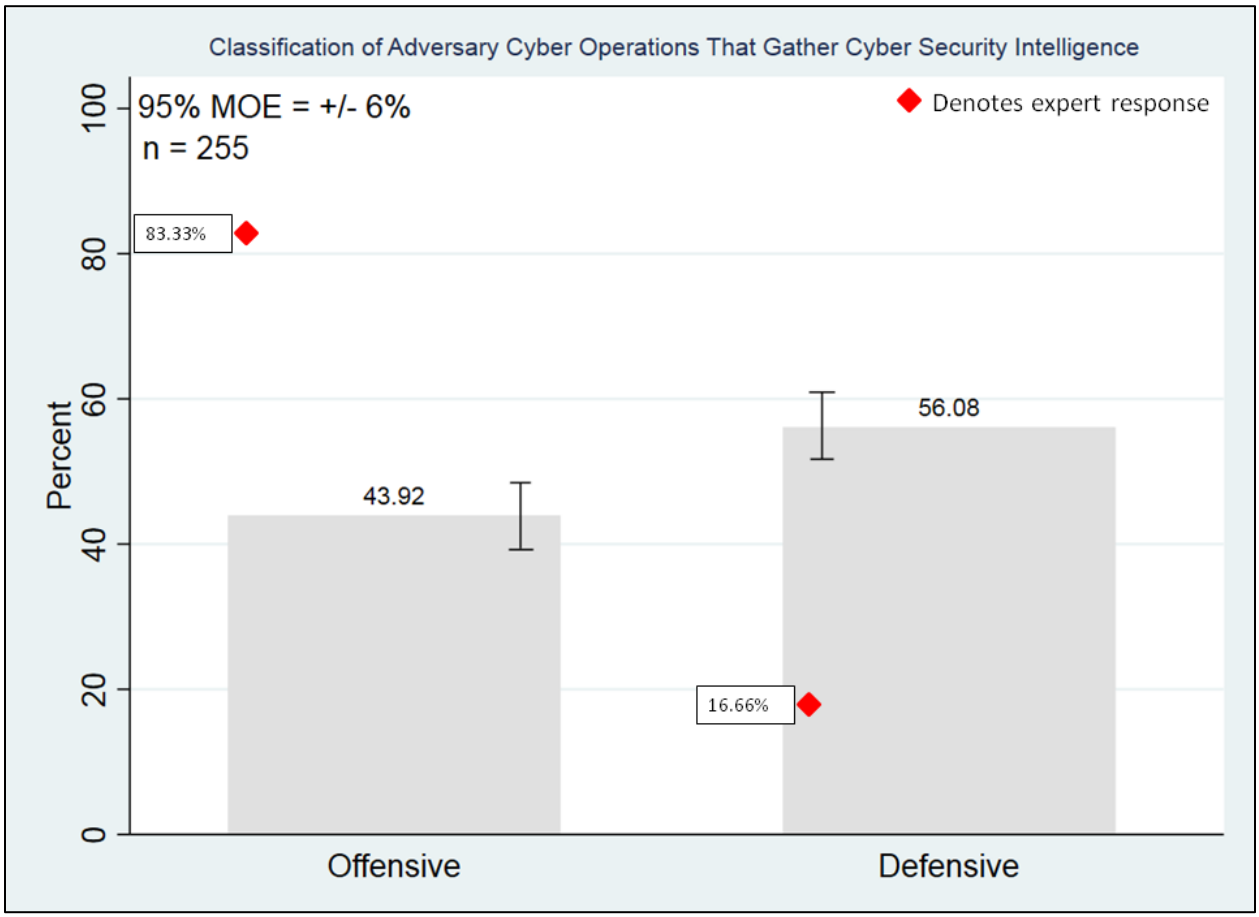


Figure 3.15 H4.2 Expert Responses

Hypothesis four is the first example of the experts differing in their responses when compared to the broader survey experiment population. The experts classified this mission as overwhelmingly offensive (83 percent), which is what the theory predicted, whereas the public

classified the mission as defensive. While the number of experts randomized into this scenario is too small to perform statistical significance tests (n=18), the results do show a definite skew in the direction predicted by the theory. If a larger sample size of experts confirmed this result, it would show that those with above-average knowledge of the cyber domain view any attack on their network as offensive in nature, as the theory predicted.

The next question tests H5 by asking respondents to select which cyber strategy they believe would be the most beneficial for the US over the next decade. The first strategy was offensive, while the second strategy was defensively focused. Figure 3.16 shows the results overlaid on the general population's responses.

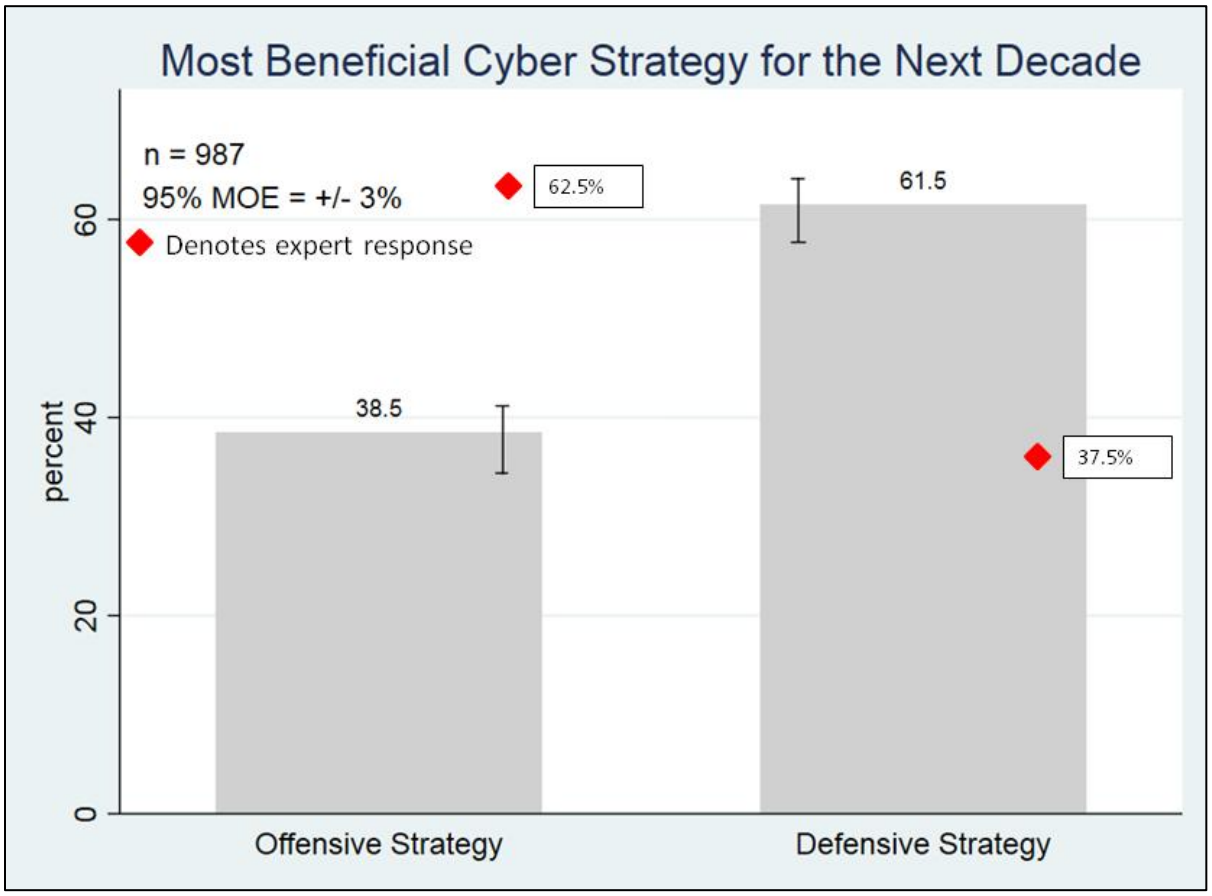


Figure 3.16 H5 Expert Responses

As with the previous hypothesis, the experts disagreed with the public and instead responded as the theory predicted. By a margin of 62.5 percent to 37.5 percent, the experts preferred an offensive cyber strategy for the US over the next decade. This question was given to all 64 respondents because there was no control or treatment group as with the previous questions. The n is larger for this question, and thus the data illicit more confidence than some of the other questions that had less respondents.

The next question tested H6 by asking respondents to choose which nation, among a group of three, was the least threatening. Each nation was identical except in how they funded their cyber forces. Nation A spent 10 percent of their cyber budget on defensive cyber forces, while Nation B spent 50 percent, and Nation C spent 90 percent. The remainder of the budget for each nation was spent on offensive cyber forces. Figure 3.17 (next page) shows the expert results overlaid on the original public responses.

Mirroring the results from the larger public survey, the experts found Nation A the least threatening nation, which provides further support for the theory's prediction that people view expenditures on offensive cyber forces as threatening, while expenditures on defensive cyber measures do not elicit feelings of threat or fear.

The next question tests H7 by asking respondents to indicate the mix of offense versus defense they desire in US Cyber policy for the upcoming decade. Using a sliding scale from 0 to 10, where 0 means purely defensive and 10 means purely offensive, respondents indicated the offensive/defensive mix the US cyber strategy should be for the next 10 years. Figure 3.18 (next page) shows the original results with the 64 expert responses overlaid in red diamonds (in percentages).

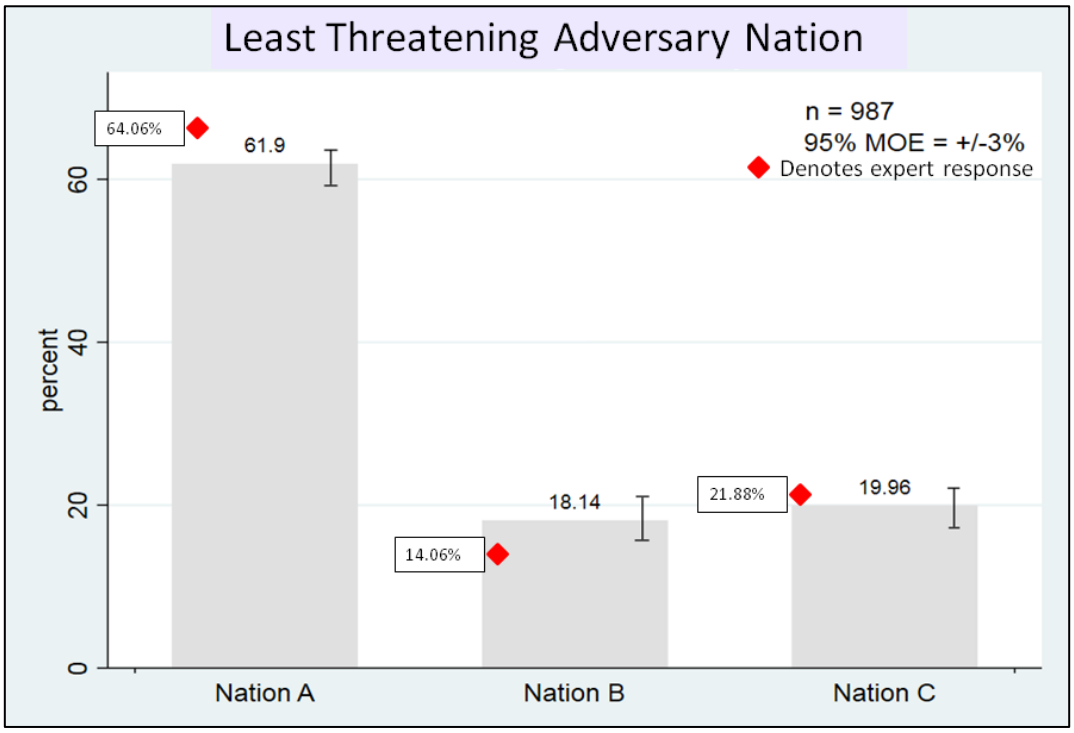


Figure 3.17 H6 Expert Responses.

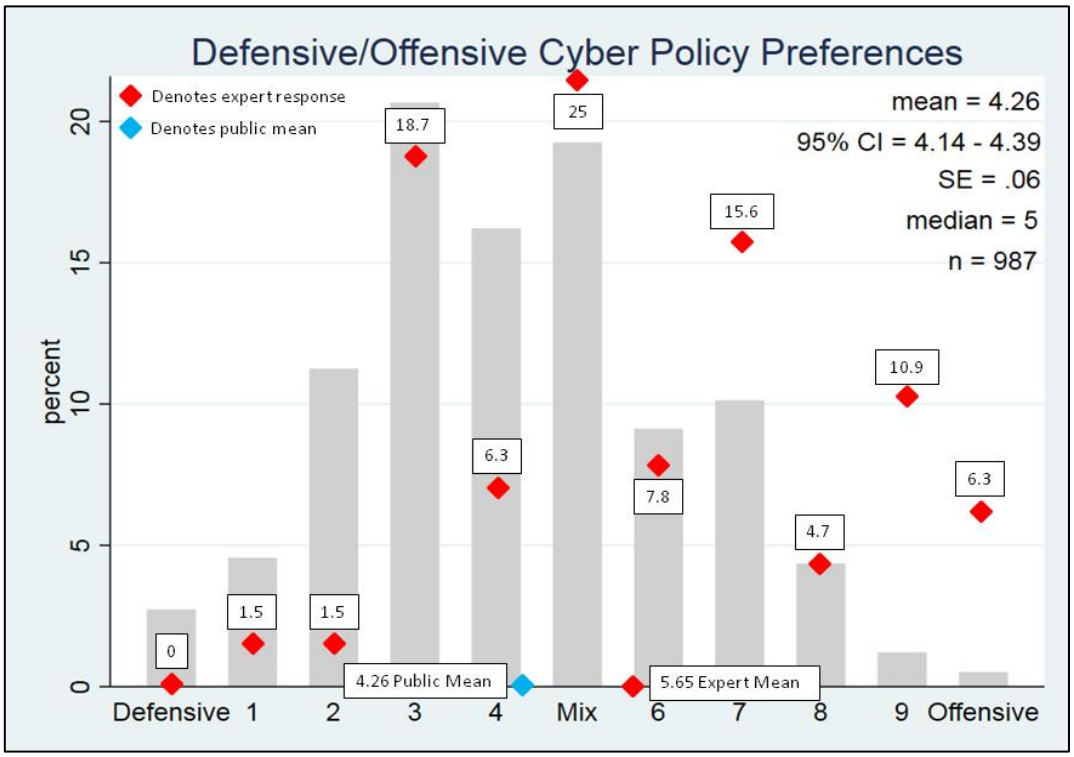


Figure 3.18 H7 Expert Responses.

Opposite of the public, but following the theory, the experts selected a more offensive strategy balance with a mean response of 5.65. With 5 being a perfect offense/defense balance, the experts preferred a more offensive strategy than the public did (public mean 4.26). As the percentages show in the black outlined boxes, experts preferred a more offensive balance (anything above 5), then a more defensive balance (anything below 5) when compared to the MTurk sample of US residents.

Discussion of the Expert Results

While the pool of respondents for the expert survey is smaller than the public survey, there are still some critical findings from this first-ever survey experiment of experts. First, the experts responded to each test exactly how the theory predicted. If a future test on a larger sample replicates these results, we could confidently say the theory is an accurate predictor for how experts view the cyber domain. The accuracy of the theory at predicting their responses has some important implications when we combine the results to paint a complete picture.

For example, the experts believe the best option (out of four) for increasing US cyber security was to offensively probe adversary networks to glean intelligence. When asked their level of support for such a cyber operation, their mean level of support was 8.38 on a 1 to 10 scale, which is near full support for such an operation. Yet, when asked how they would classify such a mission, the majority (68.5 percent) said it was a defensive mission. The result tells us that experts believe probing enemy networks is an effective way to bolster cyber security, they offer high levels of support for such operations, and they classify them as defensive.

This logic helps sustain strategic instability within the domain because all cyber operations are going to appear offensive to the nation or organization who is the subject of such an intrusion, regardless of how experts from the attacking state classify it. A 2014 National

Academy of Sciences report on cyber security highlighted this tension by noting that the US promotes cyber security on the international stage every chance it gets, but consistently undermines those goals with offensive cyber operations designed for "intelligence purposes."[183] It is also important to note that the public responded in the same manner, meaning increased public input will not likely change this issue.

Next, the experts classified any adversary's cyber attack as offensive, even when told the enemy was undertaking the attack to gather intelligence to increase their cyber security. Primarily, the experts classify their intelligence gathering missions as defensive but consider them offensive when another state executes the same type of mission. The experts diverged from the public, who remained consistent in their defensive classification of such missions, even when it was an adversary undertaking the mission against the United States.

The theory says the experts feel this way because they recognize that from a technical perspective, there is no easy way for the US to identify which attacks are simple intelligence gathering missions, and which are more problematic offensive attacks. Each requires forced access into the target network, so initially, they appear similar. The public may change their response to this question with increased engagement and dialogue with cyber policymakers.

The final difference is the experts' preference for an offensive strategy for the next decade. As with the previous hypothesis, the experts aligned with the theory and opted for an offensive strategy, while the public preferred a more defensive strategy. The ramifications of this divergence of opinion are more extreme than the previous hypothesis because this involves the strategic direction of the US government's cyber industry and forces. I theorize that the public preferred the more defensive strategy because, as outlined in Chapter One, they fear cyber

[183] National Research Council. *At the Nexus of Cybersecurity and Public Policy.* Policy Report, Washington DC: National Research Council, 2014:104-105.

attacks more than any other criminal or dangerous activity, according to Gallup polling. Thus, their preference for a defensive strategy is likely a response to that fear.

Experts preferred the offensive strategy because, as hypothesized in the theory, they believe there is no such thing as genuinely effective cyber defenses. Chapter One highlighted this by showing how open-source information states that cyber attacks have even sensitive air-gapped networks (e.g., Stuxnet, etc). Thus, experts with a better understanding of the cyber domain preferred the efficacy of the offense rather than the difficult-to-impossible task of effective cyber defenses. In either case, it remains to be seen if the public would alter their response with additional information. What the expert results show, however, is that increased knowledge of the domain creates difference preferences for cyber policy.

Conclusion

The results of the MTurk survey population and the smaller expert population lend support to the two general cyber propositions. The first proposition, drawn from the theory, states that the offense and defense are difficult to distinguish. The results of both the public survey experiment and the expert sample strongly support this proposition. The assertion in the general theory asserts that the high fear displayed by the public for cyber attacks, despite the lack of empirical evidence to support such feelings, stems from the difficulty differentiating between the offense and the defense in the cyber domain. As the results showed, people rationalize what is 'offensive' or what is 'defensive' based on whether their state is undertaking the cyber operation or whether another state is. Further, the stated objectives of the cyber intrusion dictate whether they classify their cyber missions as offensive or defensive.

Logically, this creates what former US Cyber Command chief General Keith Alexander called 'strategic instability' because what the attacking state sees as a defensive cyber mission

appears entirely offensive for the attacked state, regardless of the objective of the cyber mission. This is because a benign cyber attack designed only to gather intelligence, and not to implant any offensive cyber weapons, appears to the attacked state the same as a cyber attack that is designed to wreak havoc on public infrastructure, economic systems, public transportation systems, air traffic control networks, or a number of other sensitive networks. In each case, the attacker must first establish network access, and this network access looks nearly identical to the attacked state, regardless of the mission objectives of the attacking state.

The second theoretical proposition states that people believe in the efficacy of the offense over that of the defense. The results from the general survey population lend only partial support to this assertion. Public respondents overwhelmingly felt that a state that spends the majority of its cyber expenditures on offensive cyber forces was the more threatening state when compared to states that spent the majority of their budget on defensive cyber forces. However, when asked which strategy would best benefit the US over the next decade, public respondents preferred a slightly more defensive strategy.

As noted earlier, US residents may already feel the US has invested adequately in offensive cyber weapons and now needs to refocus on defensive measures. The expert survey population, however, fully supported the theoretical proposition as they preferred a more offensive strategy and allocation of US dollars over the next decade. The experts may hold a different position because they have more in-depth knowledge of what adversary states are capable of in the cyber domain, or because they feel that in the still-young cyber domain, it is necessary to continue to push the bounds of offensive capability in a similar manner to the early air domain, as examined in Chapter two, where early ‘experts’ in the air domain advocated for

robust offensive strategies even before any evidence existed that such a strategy would pay dividends or could cause the damage they believed it could.

In either case, the evidence collected in the two rounds of survey experiments lends full support to the first general cyber proposition and moderate support to the second proposition. The next chapter utilizes a process-tracing research format to examine the debate over US cyber policy from 1986 to 2014.

CHAPTER 4

A PROCESS-TRACING ANALYSIS IN US CYBER POLICY

Introduction and Process-Tracing Structure

The structure of this process-tracing analysis follows George and Bennett's (2005) guidance on process-tracing construction and implementation for a general explanation of the causal process. This general process-tracing approach is designed to produce findings with a higher level of abstraction than the other empirical chapters provided, and this "is consistent with the familiar practice in political science research of moving up the ladder of abstraction."[184] Besides offering a broader overview of the causal mechanisms, the process tracing analysis also explains how they manifest themselves in the real world.

The statistical analysis in Chapter Three provided a high level of detail on the theory's validity through an analysis of survey experiment data. The comparative analysis in Chapter Two delivered a slightly broader empirical test of the theory and also provided generalizability to another domain (e.g., the early air domain). The process-tracing structure of this chapter provides "a higher level of generality of explanations" to better explain, refine, and assess the theory through historical examples.[185] George and Bennett, among others, assert this is a justified approach, "just as researchers using statistical methods often create larger cells either to obtain categories of broader theoretical significance or to obtain enough cases."[186]

This analysis is not designed to provide a hard test of the argument *per se*. Instead, the higher level of the analysis presented here helps form a complete empirical analysis of the theory

[184] George, Alexander and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences.* Cambridge, MA: Harvard University Press. 2005: 211.
[185] George, Alexander and Andrew Bennett. 2005: 211.
[186] George, Alexander and Andrew Bennett. 2005: 211.

by offering an explanation of the causal mechanisms during the policy development and implementation period under investigation. King, Keohane, and Verba stipulate that a process-tracing study should include "searching for evidence - evidence consistent with the overall causal theory - about the decisional process by which the outcome was produced" and that the result from such research will "enable investigators and their readers to increase their confidence in the findings."[187] This approach, however, does not release a researcher from their responsibility to look for evidence that undermines the theory.

As noted, any irregularities or cases of non-concurrence with the theory during the decision-making processes reviewed will be highlighted and used for theory refinement. This process-tracing research format provides a different type of empirical test from those in Chapters two and three, one that adds value to the project by testing and explaining the theory from a different perspective. Additionally, it offers something beyond what statistical analysis provides and gives us insight into the "black box" of the causal mechanisms by contextualizing how they operated (or failed to) in real-world situations.[188] This chapter will capstone the empirical evaluation and application of the theory and the related causal mechanisms and will help chart a path forward for theory refinement and future research.

The two general cyber propositions tested in the process-tracing analysis are: (1) People cannot easily identify the difference between offensive and defensive cyber activity. The lack of clarity in the domain elevates fear levels because citizens and elites cannot easily recognize the intentions of cyber actors. Strategic instability ensues as states struggle to understand and counter cyber activity that does not display clear and discernible intentions as actions do in other conflict

[187] King, Gary, Robert Keohane, and Sidney Verba. *Designing Social Inquiry – Scientific Inference in Qualitative Research.* Princeton, NJ: Princeton University Press. 1994:227.
[188] Crasnow, Sharon. "Process Tracing in Political Science: What's the Story?" *Studies in History and Philosophy of Science.* 2017:7.

domains. And (2), people view national cyber defense as the status quo and not as an exploitable concept that can offer measurable gains when compared to offensive operations. This proposition proposes that people believe the offensive has the advantage, and actors will have faith in the efficacy of offensive cyber operations even before evidence exists that the espoused benefits of such offensive actions are attainable or even possible. They will do this while simultaneously putting very little faith into the defense. As shown in the empirical analysis of Chapter two, these two positions mirror closely those held about the early air domain in the early 20th century.

The process-tracing analysis tests these propositions through an examination of expert testimony, statements from elites, and scholarly work during debates leading up to several crucial cyber policy initiatives. Support for the first proposition would come from evidence of two characteristics in cyber policy debate. The first is evidence that shows cyber policies and actions sought to merge the offense and the defense into a single executable mission. Such a position would include a belief among experts that strong offensive cyber action is a foundational element of strong cyber defenses. A policy designed around this requirement would obscure the line between the offense and the defense. Additional evidence would come from experts, elites, and scholars noting that they did not understand the intent behind cyber intrusions, were confused about the objectives of such operations, or were unsure what was happening in the domain. A lack of this necessary information would show that, unlike in the air, sea, and land domain, there is little clarity between the offense and the defense in the cyber domain. Evidence of this in the decision-making process would require elites to craft effective policy for a domain that defies standard patterns of offensive or defensive analysis.

Support for the second proposition would include language and actions from experts, elites, and scholars where their decisions were based on their belief in the efficacy of the offense before empirical evidence suggests such capabilities were realistic or plausible. Proactive development and pushing technological boundaries to exploit a new domain and its associated weapons are not necessarily bad policy. Instead, this process-tracing analysis examines the evidence to determine if programs and policies were guided by the premature *belief* in offensive cyber capabilities, rather than a genuine effort to develop new cyber capabilities and assess their offensive effectiveness.

The process-tracing analysis will examine evidence to determine if either or both of the general propositions were at work during US cyber policy development and implementation during two distinct stages during the growth of the cyber domain. The examination will also search for evidence that policymakers relied on information or beliefs that run contrary to the theory. The first researched period runs from 1986 to 1998. As with the comparative analysis conducted in Chapter two, the cyber domain research for this chapter will start in 1986 because it was the year of the first sizeable cyber attack directed at government classified networks (e.g., Cuckoo's Egg attack). Shortly after the attack, the US Government (USG) introduced the first significant cyber policy action in 1988. This policy action was the creation of the Computer Emergency Response Team Coordination Center (CERT/CC or simply CERT in some literature) in November 1988. This major cyber policy event was in response to the 1988 Morris worm incident, which was the first widespread cyber attack in US history that targeted civilian and academic systems in a self-replicating fashion.

The last major US cyber policy event during this first cyber period was the creation of Joint Task Force - Computer Network Defense (JTF-CND) in December 1998. The legislation

that organized JTF-CND came as a result of several critical cyber events, including lessons learned from the Eligible Receiver exercise in 1997, the findings from the Marsh Commission in 1997, and lessons learned from the Solar Sunrise cyber attack in early 1998.

The second period for the process-tracing analysis begins in late 1998 and runs to 2014. Cyber scholar Jeff Healey identifies 1998 the true "takeoff" phase of the cyber domain, as governments, militaries, and corporations began to undertake major cyber operations while simultaneously countering increasingly sophisticated cyber attacks.[189] This second period includes policy debates over lower-level cyber policy initiatives, as well as a major cyber policy that created the US Cyber Command (USCYBERCOM) in 2009. USCYBERCOM later became one of 11 unified commands within the Department of Defense (DOD) with responsibilities for full-spectrum cyber operations across all US military branches.

The objective of the empirical process-tracing analysis of the two cyber timeframes is to determine if and how the theoretical propositions influenced debates leading to policy creation and implementation. This type of analysis is essential because the survey experiment research in Chapter three only provided insight into perceptions from US respondents as well as a limited number of cyber experts. Chapter Three does give us an indication of the theory's applicability to elites by testing the hypotheses on 64 cyber experts, but it does not explain how the causal mechanisms work during policy debate. The process-tracing analysis in this chapter will provide such an analysis.

The intent of this process-tracing study is not to examine every cyber attack in the relevant periods, but rather to single out several large cyber policy initiatives to determine if the causal mechanism appeared to have any influence during the decision making process. Regardless of the outcome of the process-tracing analysis in this chapter, it will add another

[189] Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* USA:CCSA, 2013:122.

empirical data point to support or refute the theory from a perspective unique to the empirical analysis in Chapters two and three.

Cyber Domain Period One – 1986 to 1998.

Before 1986, the debate over the growing cyber domain was simplistic and varied in scope and opinion. A 1981 article in *Financial Executive* foretold of cyber "time bombs" that corporate computer experts could plant and set to go off if they lost their job or had some other unfavorable action taken against them. These programs could destroy whole databanks and set corporations back years if senior executives did not become more involved in computer security.[190] Others disagreed, with experts testifying before Congress in 1980 that cyber attacks were exaggerated and not significant enough to warrant any new federal legislation, as Congress was contemplating at the time.[191] The divergence in opinion presented to policymakers by 'experts' stalled the policymaking process and prevented the implementation of any significant cyber policy.

The debate about cyber policy did not begin to become a serious topic until the first large cyber attack against the US took place in 1986. This attack saw a coordinated team of German hackers attempt to steal information related to President Reagan's Strategic Defense Initiative (SDI - i.e., Star Wars) from several US research facilities. The attack, nicknamed Cuckoo's Egg, was designed to collect information about the SDI program to resell to adversaries. American officials eventually arrested the hackers and sentenced them to prison.

While the attackers were successful initially, the attack did little to spur organizational change within the burgeoning global cyber enterprise and had no meaningful impact on the SDI

[190] Vohs, Dennis. "The Financial Executive's Role in Computer Security." *Financial Executive*, April 1981: 30-32.
[191] U.S. General Accounting Office. "Computer Related Fraud Current Issues and Directions." Speech given before the 40th International conference of the Institute of Internal Auditors by James Watts, Accounting and Financial Management Division. June 8th, 1981:2.

program. It did, however, elevate fear levels over the capabilities and vulnerabilities in the growing cyber domain and prompted public discussions regarding cyber security and US cyber policy. Yet this debate was sporadic, often driven by a single event that soon faded in people's memory as the world moved on to the next of a seemingly endless stream of technological breakthroughs that the new domain offered.

To highlight the infancy of US cyber policy and structure at the time of Cuckoo's Egg, Cliff Stoll's very first line in a book he wrote about the attack shortly after it occurred stated, "How do you spread the word when a computer has a security hole? Some say nothing, fearing that telling people how to mix explosives will encourage them to make bombs."[192] (Stoll was the computer technician who discovered the Cuckoo's Egg attack) Stoll's quote highlights that not only did experts not fully understand what was happening in the new domain, but they were unsure of what they should do with any information they did manage to collect about cyber operations. The US government would respond with a major cyber policy initiative shortly after Cuckoo's Egg that is viable for process-tracing analysis, but not until another cyber event highlighted, in a very public way, how susceptible the new domain was to nefarious activity.

That next attack, the Morris Worm event of 1988, trigged large scale policy changes within the USG that Cuckoo's Egg did not. Unlike Cuckoo's Egg, the Morris Worm was launched not as an attack by foreign agents, but as a scientific experiment by a graduate student at Cornell. The purpose of the computer code, created and implemented by Robert Morris of Cornell's computer science program, was designed to cause UNIX connected computers to send a message to Morris so he could create an accurate count of devices on the internet.

Up to this point, there was no precise count of the number of computers connected to the internet. Either by oversight or by design (some believe Morris intentionally designed the code

[192] Stoll, Cliff. "The Cuckoo's Egg." Doubleday Publishing, New York, NY. 1989: v.

to be malicious), the program began replicating itself. It quickly clogged the limited bandwidth available for emails and other data transfer programs. Within 12 hours of its release, the Morris Worm had bogged many Unix-based computers down so severely that only a small percentage of traffic could make it across the nascent internet.[193]

A 1989 US Government Accountability Office (GAO) report presented to Congress gave a detailed overview of the virus. The report estimated the cost from the Morris Worm, which took only two days to eradicate, at between $10,000 and $10,000,000, a range covering two orders of magnitude.[194] The apparent ease for a college student to cause such a massive slowdown in the growing internet and the inability for the government or corporations to assess the damage accurately heightened fear levels among elites. In what seems almost amusing in today's age, the 52-page 1989 GAO report refers to the Morris worm as 'the virus' because up to that point, no one had ever released a self-replicating malware program into the infant cyber domain.

This GAO report was a major part of the development of US cyber policy that eventually led to the creation of CERT, and a process-tracing analysis of the report shows that experts engaged in cyber rhetoric that, as shown in Chapter One, is still very prevalent today. The report states, "Although the virus is described as benign because apparently no permanent damage was done, a few changes to the virus program could have resulted in widespread damage and compromise…"[195] Language like this helped create the belief that the offense was potent in the cyber domain even though neither event caused much damage. As more and more experts

[193] The IEEE Computer Society. "The Morris Worm: A Fifteen-Year Perspective." *IEEE Security and Privacy*. 2003: 35
[194] US General Accounting Office. *Computer Security – Virus Highlights Need for Improved Internet Management.* Report to Congress. Washington, DC: US GAO. 1989a: 17.
[195] US GAO. 1989a:17.

proposed similar ideas, this belief became normalized and accepted by many people even before empirical evidence supported such perceptions.

As shown in Chapter One, this type of verbiage in the decision-making process is still very much at play today. Experts continually warn that every cyber attack could be the impending cyber Pearl Harbor that computer expert Winn Schwartau warned Congress of in 1991, or the cyber 9/11 that Secretary of Defense Leon Panetta cautioned about in 2012. Policy-makers quickly latched on to this language and utilized it to justify their belief that just a few different lines of code in a cyber attack could make a nearly-harmless cyber event into a potent and dangerous cyber weapon. In the case of the Morris worm, this happened despite the clear empirical evidence that the Morris worm was eradicated quickly with no permanent damage, as revealed in the GAO report.

The fact that the Morris worm did little actual damage is vital in the process-tracing analysis leading up to major cyber policy initiatives because expert opinions on the importance of the Morris worm varied widely. Some government experts saw the Morris program as an offensive weapon on the verge of creating widespread damage, yet others claimed the program was designed, albeit poorly, to count internet-connected computers with no nefarious intent. Despite the eradication of the Morris worm within days of its release and negligible losses from the Cuckoo's Egg operation, the USG responded by passing cyber legislation that created the Computer Emergency Response Team (CERT) in late 1988. (CERT is also called the CERT/CC in some literature, denoting its structure as a CERT Coordination Center)

In the aftermath of the Morris worm and the Cuckoo's Egg events, CERT was founded and funded by the DOD at Carnegie Mellon University (CMU). The objective of this new organization was to provide the USG and US businesses a central point to share information and

report vulnerabilities for the growing cyber domain. Acting as a type of first responder, CERT provided information in near-real-time about impending or recently started cyber attacks, while also sharing best practices and vulnerability fixes for computers and software. The relevant aspects of the creation of CERT are not its mission or organizational structure. Instead, a process-tracing analysis of the debating leading to the creation of CERT is where an empirical evaluation of the theory's general cyber propositions can take place.

While policymakers tasked CERT with a defensive mission, the debate about CERT's creation and implementation centered on the efficacy of the offensive potential of future cyber attacks. The theory asserts this occurred because people felt the offensive aspects of the emerging cyber domain were spectacular, even before empirical evidence existed to support such positions. While the Morris worm did cause some losses at various universities and laboratories, it hardly proved cyber weapons to be a genuinely useful and dangerous weapon. Yet the debate surrounding the creation of CERT contained rhetoric that is similar to what we see today. That is that experts always seemed to be worried about the potential offensive capabilities of cyber weapons, rather than what the empirical evidence showed was happening.

For example, Jack Brock, then director of the US Government Information and Financial Management office, testified before congress in 1989 that even though the Morris worm caused "no permanent damage" and was eradicated within two days, it "could have resulted in widespread damage and compromise" and "could have erased files on infected computers or remained undetected for weeks, surreptitiously changing information on computer files" with only "slight" changes to the worm's code.[196] As shown in Chapter one, Brock's statement to US government officials in 1989 parallels the belief in the efficacy of the offense we see today from

[196] US GAO. Statement from Jack Brock's Testimony Before the Subcommittee on Telecommunications and Finance, US House of Representatives. GAO/T-IMTEC-89-10. 1989b: 3-4.

many experts. That is, cyber weapons always appear to be on the verge of creating a cyber 9/11 or cyber Pearl Harbor even before evidence exists that such cyber events are feasible or realistic.

As the debate about CERT and its role continued in the late 1980s, belief in the offensive potential of cyber attacks was again displayed in 1989 as GAO Comptroller Ralph Carlone testified before congress about cyber attacks on NASA's Space Physics Analysis Network (SPAN). The network, initially set up in 1981, linked thousands of scientists around the world, allowing collaboration on space projects. In his testimony, Carlone stated that although NASA had no evidence of any cyber attack on the network altering or destroying scientific data, it would not be that difficult to cause damage that is "impossible to estimate."[197] As with Brock's testimony, the information given to policymakers during this period is markedly skewed by expert testimony that espoused a steadfast belief in the offensive capability of cyber attacks even as their testimony stated no such destructive attacks were occurring. This belief in the offensive power cyber attacks presented actively contributed to the optimism many had about the ability of the domain to alter future warfare, as detailed in Chapter One, and lends support to the second proposition laid out in the theory.

The theory's other proposition states that there is an unclear line between the offense and the defense, and this contributes to fear, even when the empirical evidence suggests the damage from cyber attacks does not seem to support such feelings. The GAO report to Congress on NASA's SPAN network attack captures this obfuscation when it states that the individuals who had secretly accessed the SPAN network "apparently had no destructive intent."[198] The US government was unable to determine what the intent or purpose was for all of the SPAN intrusions since there was no evidence of any data being altered, destroyed, or stolen. (While not

[197] US GAO. *Computer Security Unauthorized Access to a NASA Scientific Network*. GAO/IMTEC-90-2. 1989c:1-2.
[198] US GAO. 1989c: 2.

explicitly stated in the GAO report, the language in the report leaves open the possibility that at least some of the 'intrusions' were due to legitimate SPAN node owners granting network access to researchers without following the proper protocol, which in turn would appear as intrusions to SPAN administrators during network audits)

This same theoretical proposition is also evident in the decision-making process with the Morris worm. Government officials worried the Morris worm was a few lines of code away from being a potent offensive weapon, while Morris claimed it was a program designed to count internet-connected computers. In both the Morris worm and SPAN cases, the elevated fear levels appear front and center in policy debates before and shortly after the creation of CERT, despite no empirical evidence to support such high levels of fear.

The creation of CERT ultimately did little to quell rising fears about the problems the new cyber domain presented to policymakers. In 1991, computer security expert Winn Schwartau testified before Congress that "government and commercial computer systems are so poorly protected today that they can essentially be considered defenseless; essentially, an electronic Pearl Harbor waiting to occur."[199] Schwartau's assessment was backed up in a 1991 National Research Council (NRC) report that gave multiple reasons to believe in the potential of cyber offenses, and why defense was so difficult: the proliferation of computers into all segments of society, poor US Government policy to regulate the growing domain, inadequate hardware and software design, little-to-no use of basic security protocols by users, and little public awareness of the threat. The report stated that these conditions created a cyber domain where

[199] US Congress. "Hearing Before the Subcommittee on Technology and Competitiveness." *Computer Security.* Washington, DC: Government Printing Office. 1991: 10.

there were "few incentives to make system[s] more secure" and where network security did not increase "at a rate fast enough to match the apparent growth in threats to systems."[200]

Despite the NRC's assertion that the USG lacked effective cyber policies, there were efforts to legislate cyber security before this, including the 1986 Computer Security Act. The act required federal agencies to pinpoint systems that contained sensitive information and undertake steps to secure the systems from attacks. Yet nearly four years after the passage of the policy, a 1990 GAO report noted that "the Computer Security Act did little to strengthen computer security government wide."[201] Beyond the Computer Security Act, the CERT seemed to have little effect on cyber security as well, with Jack Brock testifying in 1991 that CERT advisories had addressed many of the common exploits used for cyber attacks, yet "despite these warnings [from CERT], these security weaknesses continue to exist."[202] Despite no cyber attack causing any widespread damage up to this point, government reports and research projects continued to stoke fear among policy-makers. For example, a 1994 US Army War College researcher noted that the US government only detected two percent (3,600) of the estimated 182,000 attacks on its networks from June 1993 to July 1994.[203]

The next major events in the 1990s that triggered widespread debate over cyber policy included lessons learned from the Eligible Receiver exercise in 1997 (ER97), the findings from the Marsh Commission in 1997, and lessons learned from the Solar Sunrise cyber attack in 1998. These events spurred the next major cyber policy initiative, the creation of Joint Task Force – Computer Network Defense, or JTF-CND, in late 1998. The Eligible Receiver exercise of 1997

[200] National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academies Press. 1991:3.
[201] US GAO. "Computer Security – Governmentwide Planning Process has Limited Impact." Report GAO/IMTEC-90-48. GAO: Washington, DC. 1990:1.
[202] US GAO. "Computer Security – Hackers Penetrate DOD Computer Systems." Report GAO/IMTEC-92-5. GAO: Washington, DC. 1991:5.
[203] Fredericks, Brian. *Information Warfare: The Organizational Dimension.* Thesis. Carlisle Barracks, PA: US Army War College. 1996: 5.

was a no-notice exercise where hackers from the National Security Agency (NSA) undertook cyber operations against critical US infrastructure, including military Command and Control (C2) networks, civilian 911 emergency phone systems, and power grids. While the details of the operation are still classified, it is widely reported that the NSA hackers were successful at penetrating nearly every network they attacked.[204]

The next event that prompted policy discussion in the 1990s was the 1997 Marsh Report. The 197-page report was produced at the direction of President Clinton, who asked for a detailed report on national infrastructure that was vulnerable to cyber attacks. The report examined how cyber attacks could impact critical infrastructure in the energy, banking, transportation, vital human services, and telecommunications sectors. The last event was the Solar Sunrise attack that occurred in early 1998. The three-week-long cyber attack, detailed in Chapter Two, occurred shortly after tensions began to escalate in the Middle East. In January 1998, Iraq barred United Nations (UN) nuclear inspectors from accessing several military sites. President Clinton responded in February by sending several thousand additional combat troops to the region. Solar Sunrise began at about the same time in February and continued for several weeks.

These three events prompted widespread debate in the USG over cyber policy and the posture the USG should take against nefarious cyber activity. In these debates, we find evidence that the theoretical propositions influenced and guided policy debate. For example, the ER97 exercise debrief report states that it is difficult to determine the threshold between simple online criminal attacks, such as hackers looking for financial gains or notoriety, and a more significant "concerted attack on the security of the United States."[205] This finding guided decision-makers

[204] Healey, Jason. 2013:42.
[205] Martell, Michael. *National Security Archives at GWU.* 2018. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations (accessed October 7, 2019).

in their process of policy development, and it supports the first general proposition that elites fear cyber attacks because of the inability to distinguish between the offense and the defense, or more generally, to determine the intentions of cyber actors.

The results and findings of the ER97 exercise spread throughout USG channels. Shortly after the release of the ER97 report, we find evidence that the first general proposition was again at work. This time, it was in response to the Solar Sunrise attack in early 1998. With the ER97 findings still fresh in policymakers' minds, Deputy Secretary of Defense John Hamre briefed President Clinton that the Solar Sunrise attacks "might be the first shots of a genuine cyber war, perhaps by Iraq."[206] As detailed in Chapter Two, the antagonists behind Solar Sunrise turned out to be several juveniles who undertook the attack for fun. While this finding was undoubtedly embarrassing for those who first thought Solar Sunrise to be a state-sponsored military attack, it also elevated fear levels among government elites as they sought to develop policies for attacks that displayed no clear intentions. The elevated fear levels among elites existed even though the evidence shows the Solar Sunrise cyber attack appears to have done little to interfere with President Clinton's or the US military's ability to respond to the issue with Iraq in 1998.

The Marsh report from 1997 also shows evidence of the first proposition at work in the policy-making process when it states, "it may be impossible to determine the nature of a threat until after it has materialized."[207] This type of assertion in policy debate causes fear because it leaves stakeholders to dream up the worst possible scenario for their area of control; it is the root of the 'cyber Pearl Harbor' and 'cyber 9/11' doomsday comments made by high-ranking government officials. Strategic instability follows because policymakers are left to craft policy for a threat that displays no definite intentions. Thus they dream up the worst possible scenarios

[206] Healey, Jason. 2013: 43.
[207] President's Report on Critical Infrastructure Protection. *Critical Foundations – Protecting America's Infrastructures.* Presidential Report, Washington, DC: White House, 1997:x.

and craft policy to deal with such predictions, despite little empirical evidence to support the fears driving their policies.

There is also widespread support for the second general proposition during this process. The proposition states that optimism is a result of people's belief in the efficacy of the offense as a game-changing medium, even before evidence suggests these beliefs are justified. For example, the Marsh report noted to policy-makers that there was no evidence of an impending debilitating attack. Interestingly, in a discussion of the ER97 exercise, the Marsh report asks, "Was [ER97] an over-statement of today's vulnerabilities or a glimpse at future forms of terrorism and war? The experience to date, the known vulnerabilities, and the continuing pace of change suggest the latter."[208] As shown in Chapters One and Two, these are not throwaway statements to policymakers; the efficacy of the offense became steadily ingrained into the decision making process of elites.

As detailed in Chapter One, the damage caused by cyber attacks (not just up to this point, but up to the present) has inflicted little actual harm on US residents. Further, despite the US creating many would-be antagonists around the world by fighting in multiple wars around the globe since the 1990s, there is no evidence that terrorists or adversaries have utilized the cyber domain in the way in which the Marsh report concluded was likely. The theory's proposition predicts this outcome because an overriding belief in the offense creates undue optimism for the domain to shape and alter conflict in a way which, up to now, has not occurred and is not empirically supported.

The Marsh report gained significant traction in the USG and influenced policymakers as they grappled with policy responses to the growing cyber domain. A process-tracing analysis of the debate and information in the report further supports the second proposition. The report

[208] President's Report on Critical Infrastructure Protection. 1997:8.

states, "A satchel of dynamite and a truckload of fertilizer and diesel fuel are known terrorist tools. Today, the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives…"[209] This type of statement rang true with policymakers because it directly implicates the safety of their constituents. As with the previously-analyzed assertion, the analysis in Chapter one found no empirical evidence to support such a claim.

The Marsh report goes further, seemingly drawing a comparison between the damage future cyber attacks could cause and the 1993 World Trade Center attack, the 1995 bombing of the Murrah federal building in Oklahoma, and the 1996 Khobar Towers bombing.[210] These three attacks killed 194 people, injured over 2,000 people, and caused untold financial losses for the USG and foreign stakeholders. Comparing cyber attacks to such events gave decision-makers a vivid visualization of the damage future cyber attacks could cause as they debated policy initiatives. This is despite empirical evidence that cyber attacks at the time of the Marsh report (and even up to the present) had caused some financial losses for business owners and governments, but no known loss of life.

There were some limited instances of experts attempting to reframe the cyber policy debate process with warnings about the rhetoric espoused during congressional hearings. In a 1999 Washington Post article written by William Arkin, an expert on national security and the internet, he stated that a little-known unit within the Pentagon called the Special Technical Operations Division (STOD) had been "trying to figure out how to hack Iraq for a long time and have found the challenge daunting."[211] This assertion flew in the face of the overriding optimism

[209] President's Report on Critical Infrastructure Protection. 1997:x.
[210] President's Report on Critical Infrastructure Protection. 1997:5.
[211] Arkin, William. *Washington Post.* January 18, 1999. http://www.washingtonpost.com/wp-srv/national/dotmil/arkin011899.htm (accessed October 7, 2019).

found in the Marsh report, the finding from ER97 and after-action reports from the Solar Sunrise event, which cast cyber operations as a somewhat painless and easy means to attack a state.

Arkin's article was in response to a December 1998 Wired.com interview where Steve Stakton, a member of the Legion of the Underground hacking group, claimed that if the group wanted to, they could "dial up and make a huge amount of connection[s] to [Iraqi] systems and possibly bring it down to its knees."[212] Stakton's comment came just a few months after another hacking group called L0pht testified before Congress in May 1998 that they could take down the entire internet in only 30 minutes.[213]

Such claims before Congress by groups like L0pht, along with those presented earlier from the USG reports, show the vast majority of discourse over cyber policy was guided by a belief in the efficacy of the offense over the defense. What is striking, however, is that Arkin sourced his article from people within the Pentagon who were acutely aware of the ability for Iraq's cyber defenses to impede any cyber attacks against their networks – a direct challenge to the 'efficacy of the offense' narrative given to policy-makers. Remarkably, the challenges the STOD unit faced hacking into a third world country's network seemed to play little if any role in the public debate over cyber policy in the late 1990s other than Arkin's Washington Post article.

Arkin noted this lack of factual information in policy debates by highlighting that a widely believed report published by US News and World Report in 1992, which detailed how the NSA had managed to implant a virus into an Iraqi printer that caused their network to crash with each use, was false. The story, Arkin says, originated in an April fool's issue of InfoWorld, yet was later reported as fact in many publications, including a book on cyber security released by

[212] Glave, James. *Crackers Set Sights on Iraq.* December 30, 1998. https://www.wired.com/1998/12/crackers-set-sights-on-iraq/ (accessed October 9, 2019).
[213] Timberg, Craig. *In 1998, these hackers said the internet would become a security disaster. Nobody listened.* June 27, 2015. https://www.dailyherald.com/article/20150627/business/150629234/ (accessed November 14, 2018)

James Adams in 2001.[214] In the 1990s, Adams founded a cyber security company called iDefense and would later testify before congress in 2000 about cyber security issues. The USG later appointed Adams to the NSA's advisory board, where he gave input on cyber security issues and policy formation.[215] This type of empirically-unfounded advice was prevalent in cyber policy discussions leading up to the creation of JTF-CND and influenced the process of policy development.

The founding documents for JTF-CND show how difficult it was for policy makers to formulate a clear objective for US cyber forces. Initial documents handed to JTF-CND leaders gave it the mission to execute "active defense" of the cyber domain.[216] Records show US Air Force lawyers wanted this language removed because the military lacked definitions for defensive actions, offensive actions, and 'active defensive' actions.[217] Such a lack of mission clarity, perhaps more than anything else analyzed thus far, provides support to the theoretical proposition that the defense and offense are challenging to distinguish in the cyber domain. While not explicitly spelled out in any of the documents reviewed for this section of the research, the term 'active defense' likely refers to a cyber defense strategy that requires constant offensive probes of the enemy to determine capabilities. The process-tracing analysis thus far has shown that this belief played a critical role in cyber policy development.

As noted in Chapter One, this type of 'active defense' mentality is likely what led the National Academy of Sciences to state in their 2014 report that the US tries to promote cyber security on the international stage every chance it gets, but consistently undermines those goals

[214] Arkin, William. 1999.
[215] Bamford, James. *Body of Secrets – Anatomy of the Ultra-Secret National Security Agency.* Double Day, New York, NY. 2001:462.
[216] Healey, Jason. 2013:45.
[217] Healey, Jason. 2013:45.

with offensive cyber operations designed for "intelligence purposes."[218] In either case, the process-tracing analysis of policy debate leading up to the creation of JTF-CND shows support for the theoretical propositions during policy formation and implementation in the 1987 to 1998 timeframe.

Cyber Domain Period Two – 1998 to 2014.

Starting shortly after the creation of JTF-CND in 1998, there were several smaller cyber policy initiatives worthy of a process-tracing analysis. In 1998, President Clinton signed Presidential Decision Directive-63 (PDD-63), which set forth a defensively-oriented cyber policy designed to "swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[219] The 18-page directive further outlined critical national infrastructure elements and delineated which government agency was responsible for each sector of the economy.

It is not clear what event, if any, spurred the creation of PDD-63. What the historical records do show, however, is that in February 1998, several months before PDD-63's release, the Department of Defense became victim to the Solar Sunrise cyber attack, detailed earlier, that compromised hundreds of computers and networks at multiple military and government research locations. Government officials described the attack as "the most serious intrusion into the United States up to that point."[220]

Although Solar Sunrise did not lead to a kinetic conflict, it did highlight the fragility of the nation's cyber systems. It also showed how cyber attacks could have an impact on decision-makers when they happen during a military crisis (e.g., the unfolding crisis with Iraq at the time).

---

[218] National Research Council. *At the Nexus of Cybersecurity and Public Policy.* Policy Report, Washington DC: National Research Council. 2014:104-105.
[219] Clinton, Bill. *PDD/NSC-63.* Presidential Decision Directive, Washington, DC. White House, 1998:2.
[220]Healey, Jason. 2013:122.

After action reports from Solar Sunrise also highlighted to government officials that "organizationally and doctrinally, no one was in charge" of the effort to stop cyber attacks and defend the nation's networks.[221] Several months later, President Clinton signed PDD-63 to establish clear responsibilities between government agencies and set long-term goals for network defense. An analysis of the document highlights a disconnect in USG cyber policy. PDD-63 required that the USG propose "a system for identifying and preventing attempted major attacks… [and develop] a plan for alerting, containing and rebuffing an attack in progress," yet this is essentially what the US government set up CERT for over a decade earlier.[222]

Aside from PDD-63, cyber policy work in the early 2000s was largely overshadowed by the growing global movement to fight terrorism post 9/11. Major global cyber policy initiatives never gained traction and left states making individual policies. The United Nations Information and Communication Technologies Task Force noted in a 2002 report that nearly all recent efforts for global agreement to combat cyber attacks and cyber crime had failed for several reasons, including dictates in the policies that were incompatible with state laws (e.g., international efforts to censor hate speech infringed on domestic free speech laws).[223]

Failure to solidify international laws against nefarious cyber activity during this time (or even to the present) did nothing to reduce the strategic instability in the domain. As noted by legal scholars Greenberg et al. in 1999, "The ambiguous state of international law regarding information warfare may leave space for the United States to pursue information warfare activities. Conversely, it may permit adversaries to attack the United States and its systems."[224]

---

[221] Healey, Jason. 2012:134.
[222] The White House. *Presidential Decision Directive/NSC-63.* Washington, DC. The White House, 1998:3.
[223] Gelbstein, Eduardo, and Ahmad Kamal. *Information Insecurity.* New York, NY: United Nations ICT Task Force, 2002:118.
[224] Greenberg, Lawrence, Seymour Goodman, and Kevin Hoo. "Information Warfare and International Law." *National Defense University ACTIS,* 1998: iii.

While world leaders were grappling with universal cyber policies, the US began a more proactive approach to security by reorganizing the JTF-CND into the Joint Task Force Computer Network Operations (JTF-CNO). The USG gave JTF-CNO the authority to exercise offensive Computer Network Attacks (CNA) alongside its traditional defensive cyber mission.[225]

As the debate about cyber policy continued at this time, the US Department of Homeland Security (DHS) issued Homeland Security Presidential Directive 7 (HSPD-7), which established a federal strategy to "identify and prioritize critical infrastructure" against future attacks.[226] The debate leading up to the implementation of HSPD-7 sounded very similar to the policy discussions of the previous two decades. At a congressional hearing in 2003, California Congresswomen Diane Watson stated that missing the warning signs of apparent cyber vulnerabilities would be as disastrous as the warning signs the US missed before the 9/11 attacks.[227] As with the previous period of review, this overriding belief in the efficacy of the offense and cyber weapons' ability to create 9/11 sized disasters helped create and sustain the feeling of optimism that drove cyber policy formulation during this time.

Despite this rhetoric, the DHS had a difficult time focusing on cyber attacks in the years following 9/11. One of the agencies folded into the DHS in the early 2000s was the National Infrastructure Protection Center (NIPC), which had been previously housed at the Federal Bureau of Investigation (FBI). Despite the calls for infrastructure protection dating back to the late 1980s, DHS disbanded the NIPC and parsed out its responsibilities among other government agencies.[228]

---

[225] Joint Task Force Global Network Operations. *JTF-CND / JTF-CNO/ JTF-DNO – A Legacy of Excellence.* Historical Report, Washington, DC: Defense Information Systems Agency, undated:6.
[226] US Department of Homeland Security. *Homeland Security Presidential Directive 7.* Presidential Directive, Washington, DC DHS, 2003:1.
[227] US Congress. "Exploring Common Criteria: Can it Assure that the Federal Government Gets Needed Security in Software?" *Committee on Government Reform.* Washington, DC US Government Printing Office, 2003:58.
[228] Healey, Jason. 2013:64.

With the lack of focus on cyber attacks at the federal level, the DOD decided to take a more proactive role in cyber offense and defense by splitting the two missions from the JTF-CNO into two distinct directorates. Offensive cyber operations would eventually reside with Joint Functional Component Command Network Warfare (JFCC-NW), which fell under the command of the NSA starting in 2004. Defensive operations would reside with the new Joint Task Force Global Network Operations (JTF-GNO), under the supervision of the Defense Information Systems Agency (DISA). While this move to separate the offense and the defense would seem contradictory to the theory's claim that the offense and defense are difficult to distinguish, a review of JTF-GNO documentation shows otherwise.

A DISA historical report that details the origins of the JTF-CNO and JTF-GNO notes that "JTF-GNO revolutionized [Computer Network Defense] by developing a computer network intrusion taxonomy that operationalized CND intelligence" and "as the recognized experts in CND intelligence support to network security, JTF-GNO improved Intelligence collection."[229] As shown in an examination of elite statements in Chapter one, there are hints that active cyber defenses required at least some offensive actions, which provides the necessary underpinnings for the theory. This unclear line between the offense and the defense is seen in other US policy debates as well.

Shortly after the creation of JFCC-NW, a Congressional Research Service (CRS) report on information operations in the context of US national security stated that computer network defense "is defined as defensive measures to protect information, computers, and networks from disruption or destruction" and that responses to cyber attacks may include "monitoring adversary computers to determine their capabilities before they attempt an [information operation] against

[229] Joint Task Force Global Network Operations, undated:9.

US forces."[230] This position provides support for the first general proposition that states the offense and defense are difficult to distinguish in the cyber domain. As postulated in the theory, this elevates fear levels because all operations appear offensive to the attacked state. The cyber attack the US may be defending itself against at any given time may be an adversary reciprocating the 'monitoring adversary computers to determine their capabilities' that the CRS report states are part of a robust cyber defensive plan. No documents reviewed for this research project mention or analyze the strategic implications of this reciprocity cycle.

A few years after the separation of the cyber offense (JFCC-NW) and the defense (JTF-GNO), the USG undertook an effort to combine all military cyber forces into a single entity known as US Cyber Command (USCYBERCOM). In testimony before congress shortly before US Cyber Command was officially stood up in 2010, General Alexander, who would become the first commander of US Cyber Command, stated that it is a "good thing that we have done here… we have brought [the offense and defense] together, merged those, and I think that is key to the success here."[231] The merging of the offense and defense within US Cyber Command further strengthened the notion that strong cyber security relies on offensive cyber operations. As outlined in the theory, the unclear line between offensive and defensive actions in the cyber domain helps create and sustain the fear we see from the domain, despite limited empirical evidence to support such feelings.

Moving into the early 2010s, core US documents and statements from public leaders during the period show a more open stance in favor of offensive as the preferred form of cyber operations. As stated in the theory, this belief in the offense is the direct source of optimism for

[230] Wilson, Clay. *Information Operations and Cyberwar: Capabilities and Related Policy Issues.* Congressional Report, Washington, DC: Congressional Research Service, 2006:4-5.
[231] US Congress. *US Cyber Command: Organizing for Future Operations.* Congressional Hearing, Washington, DC: Government Printing Office, 2010:6.

a new domain. During these debates, leaders help elevated the idea that cyber weapons should take their place alongside traditional battlefield weapons. In October 2012, Leon Panetta argued that a cyber attack "could be as destructive as the terrorist attack on 9/11."[232] Panetta further insisted that offensive cyber capabilities be utilized "in a manner that is consistent with the policy principles and legal frameworks" that apply to other combat domains.[233]

The offense-oriented language increasingly used by US decision-makers in government documents was not widely accepted as the best approach to solving cyber problems or lowing fear levels, however. Martin Libicki, then working as a senior scientist at the RAND Corporation, wrote in 2011 that "a state with nuclear weapons that is worried largely about the survival of the nation and its citizens can afford to ignore whatever relative superiority its rivals may enjoy in cyberspace."[234] Libicki further opined that the notion that a state must develop more robust offensive cyber weapons to offset potential adversaries serves no good purpose and has "little basis in theory or fact."[235]

One of the prime reasons Libicki attempted to sway elites against offensive cyber policies is because "states have little knowledge of exactly what [cyber] weapons are in the arsenal of their rivals."[236] Thus, states concerned about cyber stability should focus on defensive measures rather than active offensive operations.[237] While some aspects of the argument have merit, Libicki never addresses the counter-argument that many policy-makers and cyber experts were making at the time. That is, a state can only construct truly effective cyber defenses if they have

[232] Farnsworth, Timothy. "US Officials Detail Cyber Policy." *Arms Control Today*, 2012: 32-33.
[233] Farnsworth, Timothy. 2012: 32-33.
[234] Libicki, Martin. "The Nature of Strategic Instability in Cyberspace." *The Brown Journal of World Affairs*, 2011: 72.
[235] Libicki, Martin. 2011:77
[236] Libicki, Martin. 2011: 77.
[237] Libicki, Martin. 2011: 77.

some working knowledge of the offensive cyber tools that the adversary may employ or the general characteristics of their networks.

As the process-tracing analysis has shown, policy-makers and experts believed offensive cyber tools were the favored method for intelligence agencies to collect such intelligence. The fluidity many desired between the offense and defense created an environment where policies designed to establish norms to reduce hostile cyber attacks from adversaries were undercut by offensive cyber operations designed for defensive "intelligence purposes."[238] (e.g., all cyber operations executed to bolster cyber defenses appear offensive to the attacked state or organization)

Some researchers and elites took the opposite stance and felt the increasingly offensive language used in strategic US cyber policy was a tack in the right direction. Keith Alexander, writing in 2013 as the director of the National Security Agency (NSA) and commander of US Cyber Command, stated that the US had developed "an evolving set of capabilities and activities that have not yet reached their collective potential."[239] While Alexander touted the need for strong offensive capabilities, he always couched his argument in defensive terms. The approach of justifying offensive cyber operations as a cornerstone of a strong defense is precisely the position that the National Research Council would take issue with a year later, and is a foundational element in the theory presented in Chapter One.

As the statistical analysis of the survey experiment showed in Chapter Three, a majority (61 percent) of respondents aligned with Alexander, as they were willing to classify a cyber attack as 'defensive' if the purpose was to collect intelligence to bolster American cyber security. As noted previous, this mentality creates strategic instability because all cyber attacks appear

[238] National Research Council. *At the Nexus of Cybersecurity and Public Policy.* Policy Report, Washington DC: National Research Council. 2014:104-105.
[239] Alexander, Keith. "Defending America in Cyberspace." *The National Interest,* 2014: 18.

offensive to the attacked state or organization. The initial network penetration technique used to collect defensive intelligence very well may look identical to network penetration used for nefarious offensive purposes like planting logic bombs, undertaking network corruption, or data altering/deleting. As highlighted in the process-tracing analysis, this causes states to view all cyber attacks as offensive, even as leaders at the highest level of the attacking state rationalize their state's cyber operations as defensive 'intelligence gathering' missions.

There were also other concerns about the reorganization and operationalization of US cyber forces during this time. Alexander argued the efforts to streamline and fully operationalize US cyber forces were necessary because "the United States is striving to maintain the edge it holds over potential adversaries in cyberspace."[240] To some, Alexander's strict adherence to a defensive description was telling, given the revelations of offensive NSA cyber activity from the 2013 Snowden leaks. Harris (2014) says that Alexander designed his "bad news about weak cyber defenses" to bolster his argument "that the NSA should take a more forceful role in protecting the country."[241] Alexander's argument lends support to the proposition that elites feel that strong cyber defenses rely on intelligence-gathering cyber missions, which nearly always appear as offensive to the victim organization.

Harris continues and states that Alexander was willing to "exaggerate the cyber threat and dumb down his own agency's response" because he wanted public support for the NSA's offensive cyber capabilities.[242] As shown, those offensive cyber capabilities were a core component of US cyber policy, and Alexander said having those tools gave the US "the power to change the narrative by making our networks more secure."[243] Having the head of the NSA

[240] Alexander, Keith. 2014:23.
[241] Harris, Shane. *@War*. New York, NY: Houghton Mifflin Harcourt Publishing, 2014: 214.
[242] Harris, Shane. 2014:215.
[243] Harris, Shane. 2014:18.

opine that potent offensive cyber weapons were a critical part of secure networks undoubtedly had much sway among elites.

Alexander does not make it clear which 'narrative' he was referring to in his remarks. With the Snowden leaks only several months old, it seems reasonable to assume Alexander was trying to head off the torrent of negative press that the offensive-centric US cyber policy was under at the time. In either case, the process-tracing analysis shows support for the first general cyber proposition that asserts the offense and defense are difficult to distinguish in the cyber domain. As shown, elites rationalized cyber operations as either defensive or offensive based on their objectives and whether they are the attacker or the attacked. As asserted in the theory, this raises fear levels because virtually all cyber operations, even those required for cyber defense, appear as offensive operations to the attacked state.

One of the reasons cyber policy debates during this timeframe may have varied so widely in opinion is because of the lack of scientific research exploring such issues. More traditional aspects of the international political scene are broadly researched, and generally have empirically-grounded theories that policymakers can utilize to understand the global environment better as they develop policy. Politicians exploring the possibility of sending Foreign Direct Investment (FDI) to a state have a wealth of scientific research to rely on when deciding whether to send capital to a country or not. Another example is research examining the effectiveness and role of international peacekeeping forces. This research gives policymakers some guidelines that help shape the debate over a new policy. The process-tracing analysis shows that policymakers and government leaders rarely (if ever) relied on any scholarly research or advice in their decision-making process.

In 2013, Colin Gray noted this lack of scholarly assistance to government leaders when he opined that "the networked computer has fueled a large library on the technology and the tactics of the emerging digital age, but very little of lasting note on the strategic meaning of it all. Senior people in the ranks of strategic studies have by and large ignored the growing cyber challenge, while those who are technically highly cyber knowledgeable typically have scant background in strategy."[244] Without a scholarly foundation for much of the policy debate, process-tracing analysis shows elites engaged in rhetoric and rationalizations that best suited their desired policy outcomes, as the theory predicts. Despite this, cyber policy creation continued.

Shortly after US Cyber Command became fully operational, President Obama signed Presidential Policy Directive 20 (PPD-20) in 2013. The directive detailed critical sectors of the nation that agencies needed to prioritize from cyber attacks and specified roles and responsibilities for various government agencies concerning cyber operations. While PPD-20 is classified, the White House later released an unclassified single-page fact sheet on PPD-20 after someone leaked the full PPD-20 document. The fact sheet gives no specifics, but does note that PPD-20 is "part of the Administration's focus on cyber security as a top priority."[245] Further, the fact sheet states that PPD-20 "establishes principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools we have at our disposal."[246] Elements of the fact sheet give the impression of burgeoning US involvement in offensive cyber operations. Interestingly, the conclusion states that network defense and law

[244] Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Sky is not Falling.* Carlisle Barracks, PA: US Army War College, 2013:vii.
[245] White House. "Fact Sheet on Presidential Policy Directive 20." Washington, DC: The White House, January 2013.
[246] White House, 2013.

enforcement are the priorities and that US policy shall be to "undertake the least action necessary to mitigate threats."[247]

While the unclassified PPD-20 Fact Sheet gives guiding principles for defensive cyber operations, Harris (2014) posits that PPD-20 transformed US cyber operations in a far more fundamental way because it elevated cyber operations to the same status as traditional combat domains.[248] The policy directive instructed US agencies to no longer treat cyber as a support domain, but rather as an active medium for combat. The distinction is important because the public acknowledgment of the combat nature of the cyber domain by a world power further legitimizes its use for offensive attack operations for all states.

As the process-tracing analysis has shown thus far, the formation of these beliefs was founded in early cyber policy debates and continues unabated today. This debate closes out the examination for the period from 1998 to 2014. The process-tracing analysis for the period from 1998 to 2014 shows support for the two general propositions of the theory during the public debate over several major cyber policy initiatives.

Conclusion

The process-tracing analysis undertaken in this chapter examined critical junctures in US cyber policy development from 1987 to 2014. The results of the study showed policymakers and experts consistently engaged in debate and undertook policy action that is consistent with the theory. During the periods examined, elites routinely used language and took actions that parallel what the theory predicts. Experts routinely expressed optimism with language that indicated cyber attacks could paralyze an entire nation, kill people, shorten battles, cause widespread economic damage, or minimize the need for conventional military forces. Yet, this

[247] White House. 2013.
[248] Harris, Shane. *@War*. New York, NY: Houghton Mifflin Harcourt Publishing, 2014:56.

all occurred without any empirical evidence that such events were realistic. The limited evidence that was available, such as STOD's inability to use cyber weapons with any real effect on a third world country like Iraq, never appeared in any policy debates nor had any assessed impact on policy decisions.

Fear was expressed during policy debates by a constant juxtaposition of cyber weapons alongside devastating events like Pearl Harbor, 9/11, the first World Trade Center attack, and the Khobar Tower attack. Experts also claimed an adversary's cyber weapons could overfly traditional US military defenses and have effects similar to weapons of mass destruction. Further, the analysis showed experts and elites had a poor grasp on what was happening in the cyber domain and could not discern between offensive and defensive actions. Or, more plainly, what the intentions were behind cyber activities. Intentions were particularly difficult to ascertain during the Solar Sunrise event. A top advisor briefed President Clinton that the attack may be beginning signs of a cyber war launched by Iraq, yet just a few weeks later it was determined to be three juveniles who executed the attack for fun.

The first policy event analyzed was the creation of CERT by the USG at Carnegie Mellon University. The debate leading up to the creation of this first-ever cyber first response unit shows the policy creation process was guided by the general propositions outlined in the theory. The Morris worm incident prompted public officials to expressed widespread fear over cyber attacks, even as the empirical evidence showed the worm had a limited impact on the relatively new cyber domain. Still, government officials opined that the worm could have been far more destructive with only a few slight changes to the code. Experts also expressed optimism for cyber weapons to cause destruction greater than what any evidence at the time showed they could.

The Cuckoo's Egg attack at about the same time seemed to prompt far less public discussion over capabilities of the growing cyber domain, even though in real terms it was likely more damaging to the US than the Morris worm. In either case, the US set forth its first major cyber policy initiative in the wake of the two events with the creation of CERT. Process-tracing the debate leading up to the implementation of CERT showed that both of the propositions asserted in the theory were at work as elites made their decisions. In the discussions, the offensive efficiency of cyber attacks seemed overwhelming, and policymakers ran wild with opinions about the destructive capabilities of cyber weapons. Some even went so far as to compare future cyber attacks with the Pearl Harbor attack that killed thousands.

As the process of policy development continued after the creation of CERT, we find the theory's propositions influenced more critical policy junctures. The findings from the Marsh report, the ER97 exercise, and the Solar Sunrise event of the late 1990s showed that policymakers could not make a clear delineation between offense and defense actions. Further, the policy process was guided by elites who felt the efficacy of the offense foretold of disastrous consequences, even before any empirical evidence truly supported such feelings. This prompted US government officials to create the JTF-CND. Leaders tasked JTF-CND with the role of 'active defense' in the cyber domain, despite the unrecognizable nature of this term to military lawyers. As the theory predicts, this stems from the belief that unique attributes of the cyber domain make offensive cyber operations a prerequisite of strong defenses.

Moving into the second period examined, the process-tracing analysis shows that PDD-63 and HSPD-7 helped reorganize JTF-CND into JTF-CNO, which gave it authority to execute offensive missions alongside its traditional defensive role. Shortly after that, officials split the organization into two distinct entities: the JFCC-NW and the JTF-GNO. The historical records

show that computer defense, as defined by the CRS, required monitoring adversary networks to determine their capabilities. So while the offense and defense appeared split during this time, the process-tracing analysis shows that there was still an unclear line between what cyber offense and cyber defense meant among elites. Decision-makers responded shortly after that by merging the missions again.

The two missions were remerged into a single entity with the creation of US Cyber Command. The process-tracing analysis shows that officials often sought to couch their arguments for this policy in defensive terms, even as their organizations undertook offensive actions. The analysis also showed policy experts often displayed a strong belief in the efficacy of the offense, even though there was little evidence available at the time that showed cyber attacks could ever cause a cyber Pearl Harbor or cyber 9/11 as some believed.

In summary, the process-tracing analysis presented in this chapter does not provide evidence on its own that the theory is correct. Instead, in conjunction with the empirical evidence provided in Chapters Two and Three, it adds additional support to the theory's central claims and demonstrates how the causal mechanisms manifested themselves in policy debate. It also shows that the theory has applicability to not just US residents or experts, as shown in Chapter Three, but also to those who debate and decide upon cyber policies at the highest levels of the US government.

CHAPTER 5

CONCLUSION

Summary of the Results

The goal of this scientific research project was to determine why we observe such high levels of optimism for cyber weapons to inflict significant damage to an enemy and why such high levels of fear exist without any empirical data to support such perceptions. There has been no cyber demonstration event (e.g., a cyber 9/11) that would provide a foundation for such perceptions. Nor have cyber attacks proven their ability to alter the political calculus of state leaders or make future wars less deadly. While there have been financial losses due to cyber attacks, the data show much of the breaches that have caused such losses were due to lapses in basic cyber security (e.g., not encrypting stored credit card numbers), rather than a result of the overwhelming innate power resident in the domain.

The theory tested in this project hinges on two general propositions to explain why cyber fear and optimism exist without empirical support. First, fear arises from the inability to distinguish between the offense and the defense in the cyber domain. Lack of clarity in operational objectives causes cyber operations to appear threatening even if the state undertaking the action has no offensive intentions. A cyber weapon designed to gather intelligence as part of a defensive operation could also be used offensively to paralyze a network. It is difficult for the targeted state to discern the purpose of a cyber weapon, and even if they could, the attacker could switch the purpose of the attack quickly due to the pervasive nature of the domain. Elites and the public fear the domain because it is so difficult to grasp what is occurring. In other domains,

states can signal a defensive role for their arsenals of airplanes, soldiers, and ships with scripted defensive military exercises and preplanned training deployments. It is a straightforward process to detect a change in this posture because states can monitor the deployment of an adversary's airplanes, ships, and soldiers with reliable accuracy. The ability to discern offensive operations from defensive ones keeps fear levels in check. Because this delineation does not exist in the cyber domain, cyber operations appear threatening and cause fear regardless of the intentions of the state undertaking the cyber operation.

Next, optimism arises from a pervasive belief in the efficacy of the offense over the defense. Cyber defense is not an exploitable concept as it is in other domains. A state cannot 'deploy' anything in cyberspace to defend against an imminent attack in the same manner they can deploy ships, soldiers, or airplanes to blunt an attack in each of those domains. Further, states have nearly no warning for impending cyber attacks. Attacks in the other conflict domains are generally preceded by signals such as troop buildups or aircraft deployments. The lack of such signals in the cyber domain means cyber defense must be all-encompassing, existing everywhere at all times. Requirements for defensive omnipresence create the perception that cyber defense is the status quo rather than a form of warfare that can be decisively employed. Thus, people perceive that a potent offense is the only exploitable concept in the cyber domain. Because persistent and complete cyber defense continuously proves to be unattainable, they have great optimism for offensive cyber attacks to succeed in future conflicts.

This theory relies upon two established concepts within IR literature. In a seminal piece on cooperation under a security dilemma, Jervis (1978) explicates two variables that shape how states view threats. The first is whether state leaders can distinguish defensive weapons and policies from offensive ones. The second is whether leaders believe the offense or defense has

the advantage.[249] My theory relies on these two concepts to explain why we see elevated cyber fear and optimism without any demonstration events or empirical evidence to support such perceptions.

To validate the theory, I conducted three empirical evaluations to test various aspects of the two general propositions. The first was a comparative analysis of the modern cyber domain and the early air domain. The early air domain and the modern cyber domain exhibit nearly no similarities on the surface, yet the analysis showed they exhibited many similarities regarding perception development during their initial growth stages. The optimism for early airpower and modern cyber power to alter future conflicts played a significant role in foreign policy between states in the early years of each domain. Early airpower advocates spoke of destroying large cities in minutes or crippling economies even before aircraft could drop large munitions with any level of accuracy.

Similarly, cyber power prophets speak of the ability to ruin economies or disable vital social networks without empirical evidence that such a feat is possible. For example, former Symantec cybersecurity czar Tarah Wheeler stated in 2018 "I think that the most horrifying cybersecurity attack is going to have its own name and I think it's going to involve something more terrifying than we've thought of yet" and that "the next Pearl Harbor is going to be a cyberattack."[250]

As with optimism, the analysis showed that fear for the early air domain and the modern cyber domain were created and sustained without empirical evidence. This fear drove states to enact policies and shift budgetary resources even before evidence that national defense required

[249] Jervis, Robert and Robert Art. "*International Politics – Enduring Concepts and Contemporary Issues 6th ed.*" Addison-Wesley Educational Publishers Inc, New York. 2003:180.
[250] Turak, Natasha. *The Next 9/11 will be a Cyberattack, Security Expert Warns.* June 1, 2018. https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.html (accessed October 14, 2019).

such changes. The theory states that this fear results from a state's inability to accurately distinguish between the offensive and defensive purposes of cyber capabilities. Chapter Two showed that the early air domain produced fear because they could quickly switch the role of their aircraft from offensive to defensive with little advanced notice. Aircraft of the early air domain did not exhibit explicit offensive or defensive roles as many modern aircraft do today. General LeMay's plea to US leaders to purchase a large fleet of bombers in the 1930s for US coastal defense highlights this process as the bombers were used to firebomb Tokyo a few years later. The cyber domain mirrors this manifestation of fear because states cannot discern the purpose of another state's growing cyber arsenal.

The analysis also showed how the great optimism for the cyber domain to alter future conflict by 'overflying' traditional barriers to force employment was nearly identical thoughts about the early airplane. Yet, as I show in Chapter Two, this optimism was/is not empirically supported. In both domains, the evidence suggests that optimism exists because of the overwhelming belief in the offensive efficacy of cyber weapons. The belief in cyber's ability to bypass traditional defenses and penetrate enemy networks that control vital aspects of economic, military, and social life is identical to the belief in the early airplane and causes great optimism. Fear over the two domain periods examined existed without the empirical evidence needed to support this perception because the unique characteristics of the two domains made it nearly impossible for states to distinguish between offensive and defensive activities. The established tenets from IR scholarship on which my theory rests illustrate how this causes the fear we observe today, even without data to warrant it.

The results of the statistical analysis in Chapter Three showed support from US residents for the first theoretical proposition, and some support for the second. Cyber experts strongly

supported both propositions. The results showed that both survey experiment respondent groups felt that offensively probing an enemy in the cyber domain was a more effective way to increase cyber security than offensive probes in the air, land, or sea domain. Testing also showed that both groups gave a higher level of support to a cyber operation designed to gather cyber security intelligence versus general intelligence, which supports the proposition that the defense and offense are pliable concepts in the cyber domain. A flexible label for attacks is the driving factor behind states that regularly penetrate other state's systems for 'defensive intelligence collection,' even as those attacks appear offensive to the victim state.

Chapter Four showed that the fear and optimism expressed during cyber policy debates revolved closely around the tenets of the theory. Experts expressed fear in terms of what 'could happen' with a few changed lines of code or how the countless network penetration attempts on US networks were a sign of impending doom. The process-tracing analysis showed that there were very few times during policy debate when elites considered a more sober-minded assessment of cyber weapons. For example, I could find no instances of any experts or policymakers ever contemplating if the numerous attacks on US networks were simple 'intelligence gathering' operations, which the US was surely doing to their adversaries at the same time. Instead, the inability to grasp the intentions behind these countless cyber attacks stoked fear and drove policymakers to shape policy accordingly.

Experts also expressed optimism for cyber weapons to shape future conflicts during cyber policy debates. The process-tracing study showed elites grounded much of this optimism in the belief that the offense was the potent form of warfare for the domain, while defense seemed less beneficial. Indeed, cyber defenses were certainly considered necessary during debates. However, the need for stronger cyber defenses generally arose from the belief that the offense

was so effective in the domain. Thus, US decision-makers ramped up their offensive cyber capabilities and budgets, putting them on par with nuclear weapons both budget-wise and in their assumed role in future combat. At the same time, cyber defense development lagged behind offensive cyber development despite the constant call for better defenses. As shown in Chapter One, the majority of cyber breaches on US networks were not successful due to technical sophistication by the attacker, but rather due to network users failing to practice fundamental security procedures.

In summary, the results from the three empirical tests of the theory's two general propositions show widespread support for the first proposition and general support for the second. The test outcomes for the first proposition all showed that people had a difficult time establishing the intent behind cyber attacks, or as stated in the theory, the difference between the offense and the defense. As Jervis (1979/2003) postulated, this causes fear because "the differentiation between [the offense and the defense] allows status-quo states to behave in ways that are clearly different from those of aggressors."[251] A clear delineation between offensive and defensive actions (or weapons) produces three beneficial consequences for state leaders: (1) status quo powers can identify each other and cooperate, (2) states receive advanced warning of impending attacks because the offensive actions are identifiable, and (3) status quo states can formulate arms control agreements to limit offensive weapons.[252]

Testing showed a great inability for observers to differentiate between the offense and the defense in the cyber domain. Respondents even altered their view of what was offensive versus defensive when the survey experiment changed mission objectives or the state that was

[251] Jervis, Robert and Robert Art. "*International Politics – Enduring Concepts and Contemporary Issues 6th ed."* Addison-Wesley Educational Publishers Inc, New York. 2003:189.
[252] Jervis, Robert and Robert Art. 2003: 189.

undertaking the attack. If there is no ability to distinguish between offensive and defensive weapons and actions, then the security dilemma increases and fear abounds.

The second general proposition, which states optimism abounds because people believe in the efficacy of the offense over the defense, received support during all testing, but only mild support from the general public during the survey experiment. Jervis asserts that when the offense has the perceived advantage, states appear as aggressors and expansionists as they seek security though "the distribution of territory and influence" because there is little faith in the ability of the defense to provide the security that a state requires.[253] Such a concept helps explain much of the behavior observed in the cyber domain since its creation. State leaders have routinely expressed optimism for cyber weapons to alter future conflict and have placed great faith in the efficacy of the offense. As a result, states continue to be extremely aggressive with their cyber operations to claim cyber supremacy and increase their own security. As shown in Chapters Two and Four, leaders generally couch the need for such aggression in defensive terms.

Theory modifications

The theory performed well in all tests, except for the second proposition among the US respondent pool. These respondents supported one of the three hypotheses designed to assess the second theoretical tenet. Testing of the second proposition in Chapters Two and Four, as well as the cyber experts, all gave support to the tenet. The rationale for performing a second survey experiment on cyber experts was to determine if increased knowledge of the domain caused different reactions to the survey treatments. The observed differences between the experts and the public on two of the three hypotheses associated with the second proposition necessitate some discussion on theory modification.

[253] Jervis, Robert and Robert Art. 2003: 181.

Before beginning, it is essential to note that the expert survey pool was not large enough to allow statistical significance tests. With that said, it is still worthy of a brief discussion on the differences between the two survey pools, along with few proposals as to why the differences may exist. Further testing on a larger sample of experts can provide the empirical evidenced needed to support or refute the ideas.

Different responses between two groups of respondents for an otherwise identical test (with proper randomization among participants) can only be attributed to different traits between the two groups. In this case, the most apparent difference is the increased knowledge level of the cyber domain that the experts held versus the general population. The first hypothesis with different responses between the two groups was H5, which postulated that people believed higher levels of offensive capabilities are more advantageous than higher levels of cyber defense for the US over the next decade.

When given the option between two distinct cyber strategies, general US respondents selected the defensive cyber strategy over an offensive one as the most effective strategy for the US by a margin of 61.5 to 38.5 percent. Experts nearly exactly mirrored this, preferring an offensive strategy over a defensive one by a margin of 62.5 to 37.5 percent. Only further testing can determine precisely why a higher level of knowledge of the cyber domain causes such a shift, so I am left to only offer some possibilities for future research to examine. The first reason may be that higher levels of knowledge of the inner-workings of international politics writ large have exposed the experts to a better understanding of the intricate nature of the security dilemmas that states routinely encounter. The expert's approach and answer to the question may be rooted in their understanding of the security issues the US faces, rather than a better understanding of the cyber domain specifically.

Conversely, the general US pool may only think of their fears of the cyber domain when deciding upon an answer to the question. As shown in Chapter One, the fear levels among US survey respondents are quite high regarding cyber attacks. Thus, their inclination to opt for a more defensive strategy is likely based on personal fears, while the experts take into account the global political landscape. This same principle is likely at work with H7, where US respondents selected a slightly more defensive policy preference, on a sliding scale from 0 to 10, when compared to the experts. With zero representing a purely defensive strategy, and 10 representing a wholly offensive strategy, the US respondents had a mean response of 4.26. The experts had a mean response of 5.65.

In Chapter One, I claimed that experts would likely have a stronger adherence to the theory than the pool of US survey participants. As the results show, this is the case. The experts tacked precisely with the theory for each hypothesis. What is still up for debate, however, is if the variation is due to a better understanding of the cyber domain or a better understanding of international politics. Many of the experts surveyed do not have a deep technical understanding of the cyber domain. Instead, they are people who have been exposed to cyber issues based on their job. What nearly all of them have in common, however, is a better familiarity with the day-to-day struggles that states face with regards to security within the global environment. It seems likely that their understanding of these complicated IR issues drove them to hold fast with the tenets of the theory, versus answering the questions from a personal perspective as the general survey pool respondents likely did.

It is unclear, then, if legal scholar Peter Shane's claim that leaving the general public out of cyber policy debate is a true 'abdication' of a political leader's duty to listen to their

constituents.[254] It seems more likely that with a better understanding of the cyber domain and global politics in general, the US public may sway towards the experts versus experts trending in the direction of the US public. I base this on the fact that the experts who participated in the experiment are also members of the US public. Therefore, it seems more likely that gaining additional knowledge of the cyber domain would cause the US public to better align with the theory, rather than assuming the experts would change their positions if they better listened to the public when considering cyber policy.

Challenged Theories

To date, this is the first cyber research grounded in survey experiment data. Most of the cyber literature examined in Chapter One uses either aggregate level cyber attack data or are based on the researcher's opinions of cyber issues. No works reviewed in this project utilized empirical findings to first set micro-foundations for broader cyber theories. The unique nature of this research presents challenges for some of the assumptions in prior research. For example, Valeriano and Maness (2015) analyze the Dyadic Cyber Incident and Dispute (DCID) dataset and find support for their theory that cyber attacks are generally limited to regional neighbors and that restraint dynamics limit a state from undertaking more cyber attacks. The DCID dataset, however, only contains 192 cyber incidents between rivals from 2001 to 2011. The dataset leaves out the untold number of 'intelligence gathering' operations that often appear offensive to a state. Thus, the authors are implying that states can differentiate between the offense and the defense, or more plainly, can discern intentions. This ability to calculate intentions drives the logic of regionalism and restraint they propose in their theory. Data from this research project show that this is not a reliable assumption.

[254] Shane, Peter. "Cybersecurity Policy as if "Ordinary Citizens" Mattered: The Case for Public Participation in Cyber Policy Making." *Information Society*. 2012:433-434.

My results also undermine research works that rely on the 'rhetoric' argument to explain the fear and optimism for the cyber domain. Researchers who underpin their work with the 'rhetoric' argument (Clarke and Knake 2010 and Kello 2013) generally believe that hype from experts about the devastation of a looming cyber war creates the elevated levels of fear we observe today. Researchers believe this rhetoric occurs for several reasons, including the lack of understanding of the domain by policymakers (Walt 2010), or because elites want to over-dramatize and over-simplify cybersecurity risks (Quigley, Burns, and Stallard 2015), or because experts do not understand what a weapon is supposed to accomplish in war (Rid 2013). Regardless of the exact reason, such rhetoric leads to a situation where experts are unable to determine what is "fact or fiction, or, since they are unwilling to dismiss the threat completely, how long it is likely to remain fiction."[255] As a result, policymakers must "navigate the rocky shoals between hysterical doomsday scenarios and uniformed complacency" when trying to create sound public policy.[256]

As pointed out in Chapter One, the issue with this theoretical proposition is that the same causal mechanism does not appear to work for other domains or weapons. The prime example is how the vast rhetoric about terrorism in the post-9/11 environment only caused Gallup fear levels for terrorism to max out at 47 percent.[257] The historical range for this metric is generally 30-40 percent both before 9/11 and in the years after the attack. Thus, a lack of generalizability for the rhetoric argument casts doubt on the veracity of the theoretical claim. The source of optimism and fear tested in this project shows generalizability to other domains, is empirically supported

[255] Cavelty, Myriam. "Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology and Politics,* 2007: 20.
[256] Cavelty, Myriam. 2007: 31.
[257] McCarthy, Justin. "Americans' Worries About Most Crimes Similar to 2015." *Gallup*. November 14, 2016. http://news.gallup.com/poll/197444/americans-worries-crimes-similar-2015.aspx (accessed May 30, 2018).

and provides firmer micro-foundations for cyber theories when compared to the rhetoric hypothesis.

The last theoretical tenet that this research calls into question is the notion that cyber optimism and fear are rational, given the prior use of cyber weapons. Generally, researchers who advocate for this theory believe that the interconnectedness of people, businesses, and governments provides powerful nodes between states that reduce the need for conventional forces (Clarke and Knake 2010). The dependence on the domain for everything from banking to military command and control orders allows precise cyber attacks to paralyze networks of choice with disastrous effects (Zheng 2015). This interconnected world and the previous success of cyber operations give cyber attacks "fantastically game-changing" capabilities that naturally and rationally create optimism and fear for the cyber domain.[258]

Yet the goal of warfare is to compel your enemy to do your will (Stone 2013). And the previous use of cyber weapons has shown little-to-no ability to compel an adversary in the same manner as traditional methods of conflict. Theoretically connecting cyber fear and optimism to their previous use seems a stretch given the empirical record of death and destruction that cyber attacks have caused. We have no empirical evidence of cyber's strategic ability to coerce governments, ruin economies, or kill people. If the objective of all actions in war is to create a political reaction or change (Mahan 1890; Corbett 1911; Fuller 1926), then optimism and fear for a new weapon should be rooted in evidence that the weapon can bring about such change. Without the proven ability to cause such change, theories that hinge upon the previous use of cyber weapons as the central mechanism for fear and optimism do not withstand the rigors of the scientific process.

[258] Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar – What Everyone Needs to Know.* New York, NY: Oxford University Press, 2014:133.

Questions for future research

Any theory and its associated empirical findings need to be examined, replicated, and debated before it should be accepted as a viable theoretical alternative. Challenging the assumptions and findings presented in this research project should be the priority before moving on to additional questions raised by the work. For the moment, I will assume that my findings withstand the rigors of scientific cross-examination so that I can offer some initial areas for future research.

The first area deserving of further research is examining and explaining the difference between the cyber experts and the US population. Increasing the size of the expert survey experiment respondent pool would first allow us to validate the results with statistical significance tests. If the results hold on a larger sample, future research needs to discover why this divergence exists between the two survey populations. I proposed that the difference may be due to the experts' better knowledge of the security dilemma or global politics. The desire for experts to select a more offensive US cyber strategy versus the defensive strategy preferred by the public may also be because the experts feel less vulnerable to cyber attacks due to their (possibly) better understanding of basic internet security habits. Given the evidence presented in Chapter One that shows that a majority of cyber breaches could have been prevented with better basic security protocols, this appears to be a valid alternative worthy of further research.

One possible method to determine the source of the difference would be to rerun the survey experiment but provide some additional information about cyber attacks (the type of information our experts likely had) to the respondents before allowing them to answer questions. If there is a statistical difference between the responses collected for this project and the new data, it will give us a better idea about the source of the variation between the survey pools.

Lastly, with fear and optimism driving much foreign debate, it is a worthwhile scientific goal to determine when the elevated levels of fear and optimism for cyber weapons may subside. Or put another way, when will the perceptions 'catch up with the empirics' of cyber weapons. Chapter Two showed us that fear and optimism grew in nearly identical fashions for the early air domain and the modern cyber domain. The generalizability of the theory to the air domain means that we can utilize the early air domain as a proxy for this question. Research that explicates the causal mechanism that helped quell the fear and optimism for early aircraft may offer some valuable insight into the requirements needed to reduce perceptions that exist without an empirical foundation in the cyber domain.

Chapter Two's comparative analysis of the early air domain stopped in 1939 because, after this year, WW2 gave us a vast quantity of data from which to make more accurate judgments about the efficacy of the airplane in combat. I purposefully delimited the post-1939 timeframe in the comparative analysis because the goal was to determine the source of perceptions sans large amounts of data needed to support or refute them. It seems most likely that WW2 acted as a 'demonstration' event for the airplane, which in turn helped create more logical perceptions about the aircraft's ability to alter warfare. If proven true, it may mean that we will observe high levels of fear and optimism for cyber weapons until some event unleashes a volley of robust and sustained cyber attacks during large-scale combat. Whether these cyber attacks kill people, ruin economies, or alter the political calculus of state leaders may well determine the level of optimism and fear that exist post-conflict and into the future.

The last question worthy of further examination is the null finding for H4.2 with the general public. Hypothesis 4.2 asked the respondents to classify an adversary cyber operation designed to gather cyber security information as either offensive or defensive. The hypothesis

stated that it would be considered offensive, yet the public classified it as defensive by a slim margin. The experts answered as theorized. The finding is exciting because the general public classified an adversary's cyber operation as offensive when they were told it was designed to collect general intelligence, yet merely flipping the objective of the adversary's objective to gathering cyber security intelligence prompted the public to reclassify the mission.

As explained in Chapter Three, this does not undermine the theory because it is an unrealistic assumption that one would know the adversary's intent when a cyber attack occurs. Asking the question, however, gives us some previously unknown insight into public perceptions of cyber attacks and prompts the need for further investigation. It is plausible that the higher level of knowledge possessed by the experts led them to answer as predicted. Postulating this as an option presents an interesting dilemma, however. Experts are happy to talk about the myriad of cyber attacks that US network operations must defend against daily, and they will classify all of them as offensive regardless of the adversary's objective.

Yet when asked to classify US cyber operations, they classified operations designed to gather cyber security intelligence as defensive. Experts essentially want to have their cake and eat it too. This position is at the root of a primary concern highlighted in a 2014 National Academy of Sciences report. The authors noted the US promotes cyber security on the international stage every chance it gets but consistently undermines those goals with offensive cyber operations designed for "intelligence purposes."[259] In effect, the experts are helping to sustain a logic that prevents the creation of norms against cyber weapon use, while the public's responses would help to end this cycle. As with the previous discussion, more research is needed

[259] National Research Council. *At the Nexus of Cybersecurity and Public Policy.* Policy Report, Washington DC: National Research Council, 2014:104-105.

to determine if the public would align with experts with additional knowledge of the cyber domain.

Conclusion

The driving puzzle behind this scientific research project was why elevated levels of fear and optimism exist without empirical support. Data show policymakers and the public alike fear cyber attacks at rates higher than conventional forms of attack (e.g., terrorism, violent crime). Yet the data show cyber weapons have displayed only limited abilities to inflict harm. Nearly all of the most serious cyber attacks had little lasting impact on the victim. Even the most technically-advanced cyber attack known to date, Stuxnet, did not have any major impact on Iranian nuclear production according to the International Atomic Energy Association (IAEA).[260]

Similarly, the harm inflicted on the average US citizen is negligible. Data show the average American in 2014 was nearly as likely to be a victim of rape, murder, armed robbery, or another violent crime as they were to be a victim of a cyber attack that cost more than $100 in out-of-pocket expenses. Despite this, Americans fear cyber attacks at a rate approximately three times higher than they fear violent crimes.

Mirroring this fear are high levels of optimism for the cyber domain to alter future conflict. Chapters One, Two, and Four outlined the optimism experts and elites held and continue to hold for the domain to 'overfly' the battlefield during future conflicts. This optimism pervades policy discussion up to the highest levels of government. The manifestations of such perceptions are the creation of US government cyber entities that rival the US nuclear triad in scope and importance. As with fear, however, there is little data that would support such a perception.

[260] Sanger, David. 2012b: 206.

The objective of this dissertation was not to determine if cyber weapons should or should not be feared. Nor was it to ascertain whether cyber weapons will alter future conflict. In short, the goal was not to criticize or justify the optimism and fear people feel. Instead, the objective was to determine why these perceptions exist without a solid foundation of data. Utilizing established concepts within IR literature, I offered and tested a theory that illuminates previously unresearched causal mechanisms at work within the domain. The foundation of the theory rests on two general propositions. The first is whether state leaders can distinguish defensive weapons and policies from offensive ones. The second is whether leaders believe the offense or defense has the advantage.[261] My theory relies on these two concepts to explain why we see elevated cyber fear and optimism without any demonstration events or empirical evidence to support such perceptions.

Three empirical tests employed in this project examined various aspects of the theory. Each set of results indicated strong support for the first proposition and general support for the second. Researchers and policymakers now have the first-ever cyber theory that is rooted in data collected from a survey experiment. Previous cyber research that used individual-level data relied on standard survey data (e.g., Gallup). Such data leaves much to be desired because these data can only tell us what someone believes, but not why they believe it or what may cause them to change their position. The survey experiment in this project expands the realm of scientific knowledge by overcoming this small but important limitation.

Additionally, many other cyber research works utilize aggregate level cyber attack data. While this is a valid approach for certain research questions, such studies must be complemented with theories that explore and test the micro-foundations of assumptions, perceptions, and beliefs

[261] Jervis, Robert and Robert Art. "*International Politics – Enduring Concepts and Contemporary Issues 6th ed."* Addison-Wesley Educational Publishers Inc, New York. 2003:180.

of the actors. The level of granularity in the data and findings presented here makes a small but important step in setting these micro-foundations, and ultimately, contributing to the body of scientific knowledge.

.

Bibliography

Aldrich, John, John Sullivan, and Eugene Borgida. "Foreign Affairs and Issue Voting: Do Presidential Candidates "Waltz Before A Blind Audience?"." *American Political Science Association*, 1989: 123-141.

Aleksandrowicz, Tomasz. "Cyberspace as a Source of Threat to National Security: An Attempt to Conceptualize the Problem." *Internal Security*, 2015: 187 - 204.

Alexander, Keith. "Defending America in Cyberspace." *The National Interest*, 2013: 18-24.

Andres, Richard. "Inverted-Militarized-Diplomacy: How States Bargin with Cyber Weapons." *Georgetown Journal of International Affairs*, 2014: 119 - 129.

Arena, Philip, and Scott Wolford. "Arms, Intelligence, and War." *International Studies Quarterly*, 2012: 351 - 365.

Arkin, William. *Washington Post.* January 18, 1999. http://www.washingtonpost.com/wp-srv/national/dotmil/arkin011899.htm (accessed October 7, 2019).

Arquilla, John. *Deterrence after Stuxnet.* August 4, 2015. http://cacm.acm.org/blogs/blog-cacm/190371-deterrenceafter-stuxnet/fulltext (accessed June 8, 2018).

—. "Cyber is Already Upon Us." *Foreign Policy*, March/April 2012.

Arquilla, John. "The Strategic Implications of Information Dominance." *Strategic Review*, 1994: 24 - 31.

Art, Robert, and Kenneth Waltz. *The Use of Force.* Lanham, MD: Rowman and Littlefield Publishers, 2009.

Art, Robert, and Robert Jervis. *International Politics.* New York, NY: Addison-Wesley Educational Publishers, 2003.

Bamford, James. *Body of Secrets - Anatomy of the Ultra-Secret National Security Agency.* New York, NY: Doubleday , 2001.

Barsashka, Ivanka. "Are Cyber Weapons Effective?" *The RUSI Journal*, 2013: 158.

Bedard, Mathieu. "The Underestimated Economic Benefits of the Internet." *MEI.* March 31, 2016. https://www.iedm.org/59576-the-underestimated-economic-benefits-of-the-internet (accessed May 17, 2018).

Bender, Jeremy. "Israel: Cyber is a Bigger REvolution in Warfare than Gunpowder." *Business Insider.* February 4, 2014. http://www.businessinsider.com/the-internet-is-the-next-battlefield-2014-2 (accessed May 11, 2018).

Betz, David, and Tim Stevens. "Analogical Reasoning and Cyber Security." *Security Dialogue*, 2013: 147 - 164.

Biddle, Tami. *Rhetoric and Reality in Air Warfare.* Princeton, NJ: Princeton University Press, 2002.

Biddle, Wayne. *Barons of the Sky.* Baltimore, MD: Johns Hopkins University Press, 2001.

Brenan, Megan. *Cybercrimes Remain Most Worrisome to Americans.* November 9, 2018. https://news.gallup.com/poll/15370/party-affiliation.aspx (accessed March 22, 2019).

Broad, William, John Markoff, and David Sanger. "Israel Tests on Work Called Crucial in Iran Nuclear Delay." *NY Times* (NY Times), 15 January 2011.

Brock, Jack, interview by US House of Representatives Subcommittee on Telecommunications and Finance. *Statement of Jack Brock* (July 20, 1989).

Brodie, Bernard. *Strategy in the Missile Age.* Santa Monica: RAND Corporation, 1959/2007.

Buhrmester, Michael, Tracy Kwang, and Samuel Gosling. "Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?" *Perspectives on Psychological Science*, 2011: 3 - 5.

Byman, Daniel, Matthew Waxman, and Eric Larson. *Air Power As a Coercive Instrument.* Santa Monica, CA: RAND, 1999.

Cavelty, Myriam. "Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology and Politics*, 2007: 19 - 36.

Choucri, Nazli. *Cyberpolitics in International Relations.* Cambridge, MA: MIT Press, 2012.

Clark, David, and Susan Landau. "Untangling Attribution." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, by National Academies, 25-40. Washington DC: National Academies Press, 2010.

Clarke, Richard, and Robert Knake. *Cyber War: The Next threat to National Security and What to do About it.* New York, NY: HarperCollins, 2010.

Clayton, Mark. "The New Cyber Arms Race." *Christian Science Monitor*, 7 March 2011.

Clements, Ben. "Public Opinion in Britain Towards Military Action in Libya: A Micro-Level Analysis." *Politics*, 2012: 109 - 119.

Clinton, President Bill. *PDD/NSC-63.* Presidential Decision Directive, Washington, DC: White House, 1998.

Clodfelter, Mark. *The Limits of Air Power - The American Bombing of Noth Vietnam.* Lincoln, NE: University of Nebraska Press, 2006.

CNN. *Lawmakers Remain Distrustful of Saddam Hussein.* February 23, 1998. http://www.cnn.com/ALLPOLITICS/1998/02/23/iraq.react/ (accessed July 15, 2017).

Collier, Basil. *A History of Air Power.* London: Weidenfeld and Nicolson, 1974.

Crasnow, Sharon. "Process Tracing in Political Science: What's the Story?" *Studies in History and Philosophy of Science*, 2017: 6-13.

Crespi, I. *Polling on the Issues, Ed A.H. Cantril.* Cabin John, MD: Seven Locks Press, 1980.

CSIS-Mcafee. *Net Losses: Estimated the Global Cost of Cybercrime.* Annual Report, Washington DC: Center for Strategic and International Studies, 2014.

Darling, Lt Col Paul. "Joint Targeting in Counterinsurgency Operations ." *Air & Space Power Journal*, 2012: 49-56.

Department of Justice. *justice.gov.* May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (accessed November 6, 2017).

Douhet, Giulio. *The Command of the Air.* Tuscaloosa, AL: University of Alabama Press, 2009.

Dubin, Rhys. *Foreign Policy.* September 18, 2017. http://foreignpolicy.com/2017/09/18/u-s-trade-representative-slams-china-wto-in-rare-public-appearance-lighthizer-nafta/ (accessed November 6, 2017).

Emme, Eugene. *The Impact of Air Power.* Princeton, NJ: D. Van Nostrand Company, Inc., 1959.

Farnsworth, Timothy. "U.S. Officials Detail cyber Policy." *Arms Control Today*, 2012: 32 - 33.

Federal Bureau of Investigation. "FBI Releases 2014 Crime Statistics." *FBI.gov.* September 28, 2015. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2014-crime-statistics (accessed May 25, 2018).

Fickenscher, Lisa. *NY Post.* September 8, 2017. https://nypost.com/2017/09/08/credit-card-fraud-spikes-after-equifax-cyber-attack/ (accessed May 24, 2018).

Forsyth, James, and Billy Pope. "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace." *Strategic Studies Quarterly*, 2014: 112 - 128.

Fritzsche, Peter. *A Nation of Flyers: German Aviation and the Popular Imagination.* Cambridge, MA: Harvard University Press, 1992.

Gallup. *2016 Election Poll.* January 2016. http://www.gallup.com/poll/188918/democrats-republicans-agree-four-top-issues-campaign.aspx (accessed April 16, 2017).

Gartzke, Erik. "The Myth of Cyberwar." *International Security*, 2013: 41 - 73.

Gertz, Bill. *The Washington TImes - Top Gun Takeover.* March 13, 2014. http://www.washingtontimes.com/news/2014/mar/13/f-35-secrets-now-showing-chinas-stealth-fighter/ (accessed December 2, 2016).

Glave, James. *Crackers Set Sights on Iraq.* December 30, 1998. https://www.wired.com/1998/12/crackers-set-sights-on-iraq/ (accessed October 9, 2019).

Gollin, Alfred. *The Impact of Air Power on the British People and Their Government.* London: Macmillan, 1989.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, 2010: 102 - 135.

Gorman, Siobhan. *Wall Street Journal.* April 22, 2013. http://www.wsj.com/articles/SB10001424127887324345804578424741315433114 (accessed December 2, 2016).

Government Accountability Office. *Defense Department Cyber Efforts: DOD Faces Challenges in its Cyber Activities.* Report to Congress, Washington, DC: GAO, 2011.

—. *Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information - High Risk Issue.* 2017. https://www.gao.gov/highrisk/ensuring_the_security_federal_government_information_systems/why_did_study (accessed November 8, 2018).

Government Accounting Office. *Computer Security - Governmentwide Planning Process Has Limited Impact.* Congressional Report, Washington, DC: GAO, 1990.

Graham, Bradley. "U.S. Studies a New Threat: Cyber Attack." *washingtonpost.com.* May 24, 1998. http://www.washingtonpost.com/wp-srv/washtech/daily/may98/cyberattack052498.htm (accessed May 12, 2018).

Graham, David, and Ulrike Richardson. *Computer Crime and Security: An Annotated Bibliography of the Periodical Literature.* GAO Report, Washington, DC: GAO, 1984.

Gray, Colin. *Making Strategic Sense of Cyber Power: Why the Sky is not Falling.* Carlisle Barracks, PA: US Army War College, 2013.

Greenberg, Lawrence, Seymour Goodman, and Kevin Hoo. "Information Warfare and International Law." *National Defense University ACTIS* , 1998: 1-59.

Hagan, Shelly. "Cyber Hacks Cost up to $109 Billion in 2016, U.S. Estimates." *Bloomber.* February 18, 2018. https://www.bloomberg.com/news/articles/2018-02-16/cyber-hacks-cost-as-much-as-109-billion-in-2016-u-s-estimates (accessed May 16, 2018).

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber SEcurity, and the Copenhagen School." *International Studies Quarterly*, 2009: 1155 - 1175.

Harris, Shane. *@War.* New York, NY: Houghton Mifflin Harcourt Publishing, 2014.

Hathaway, Oona, et al. "The Law of Cyber-Attack." *California Law Review*, 2012: 817 - 885.

Hauser, David, and Norbert Schwarz. "Attentive Turkers: MTurk particpants perform better on online attention checks than do subject pool participants." *Behavior Research Methods*, 2016: 400 - 407.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* USA: CCSA, 2013.

Hughes, Jennifer, Abigail Camden, and Tenzin Tangchen. "Rethinking and Updating Demographic Questions: Guidance to Imporve Descriptions of Research Samples." *Psi Chi Journal of Psychological Research*, 2016: 138-151.

Hunn, James. "Popular Science in Paris in the 1780s: The Example of Ballooning." Unpublished Paper, 1981.

Hyde, Susan. "Experiments in International Relations: Lab, Survey, and Field." *Annual Review of Political Science*, 2015: 403-424.

Ikenberry, G. John. *Liberal Leviathan.* Princeton: Princeton University Press, 2011.

Institute for the Analysis of Global Security. *How Much did the September 11 Terrorist Attack Cost America?* 2004. http://www.iags.org/costof911.html (accessed May 30, 2018).

J. Boone Bartholomees, Jr. *National Security Policy and Strategy.* U.S. Army War College, 2010.

Jeff Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Vienna, VA: Cyber Conflict Studies Association, 2013.

Joint Task Force Global Network Operations. *JTF - CND / JTF - CNO / JTF - GNO - A legacy of Excellence.* Historical Report, Washington, DC: Defense Information Systems Agency, undated.

Jones, Jeffrey. *Gallup Polling.* November 2, 2011. http://www.gallup.com/poll/150497/three-four-americans-back-obama-iraq-withdrawal.aspx (accessed July 13, 2017).

Kavanagh, Camino. "Cybersecurity, U.S. Foreign Policy, and a Changing Landscape: A New Generation Speaks Out." *American Foreign Policy Interests*, 2014: 44 - 53.

Kello, Lucas. "The Meaning of the Cyber Revolution." *International Security*, 2013: 7 - 40.

Kellstedt, Paul M., and Guy D. Whitten. *The Fundamentals of Political Science Research.* New York, NY: Cambridge University Press, 2009.

Kennett, Lee. *The First Air War- 1914-1918.* New York: Simon and Schuster, 1991.

Lewis, James. *Rasing the Bar for Cybersecurity.* Technology and Public Policy Report, Washington, DC: Center for Strategic and International Studies, 2013.

Lewis, James. *The Cyber War Has Not Begun.* Washington, DC: CSIS, 2010.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, 1999.

Libicki, Martin. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009.

Libicki, Martin. "The Nature of Strategic Instability in Cyberspace." *The Brown Journal of World Affairs*, 2011: 71-79.

Libicki, Martin. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly*, 2014: 23 - 39.

Lindsay, Jon. "Stuxnet and the Limits of Cyber Warfare." *Security Studies*, 2013: 365 - 404.

Lindsay, Jon, and Tai Cheung. "From Exploitation to Innovation." In *China and Cybersecurity*, by Jon Lindsay, Tai Cheung and Derek Reveron, 51 - 86. New York: Oxford University Press, 2015.

Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.* Cyber Intelligence, Virginia: Mandiant, 2013.

Markoff, John. *Computer Intruder is Found Guilty.* January 23, 1990. https://www.nytimes.com/1990/01/23/us/computer-intruder-is-found-guilty.html (accessed November 12, 2018).

Martelle, Michael. *National Security Archives at GWU.* 2018. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations (accessed October 7, 2019).

Martemucci, Matteo. "Unpunished Insults - The Looming Cyber Barbary Wars." *Case Western Reserve Journal of International Law*, 2015: 53 - 62.

Mayer-Schonberger, Viktor, and Kenneth Cukier. *Big Data.* New York, NY: Boughton Mifflin Harcourt Publishing Company, 2014.

McClendon, R. Early. *The Question of Autonomy for the U.S. Air Arm, 1907-45.* Maxwell, AFB AL: Air University Press, 1950.

McFarland, Marvin. *The Papers of Wilbur and Orville Wright - Vol II - 1906-1948.* New York, NY: McGraw-Hill Book Company, 1953.

McGraw, Gary. "Cyber War is Inevitable (Unless We Built Security In)." *The Journal of Strategic Studies*, 2013: 109 - 119.

Mitchell, William "Billy". *Winged Defense.* Tuscaloosa, AL: University of Alabama Press, 2009.

Money, Art. *CTOVision.* Regularly updated. https://ctovision.com/cyber-security-wake-up-calls-for-the-federal-government/ (accessed May 12, 2018).

Morrow, John. "The First World War, 1914-1919." In *A History of Air Warfare*, by John Olsen, 3-25. Dulles, VA: Potomac Books, 2010.

Mueller, John, and Mark Stewart. "The Terrorism Delusion: America's Overwrough Response to September 11." *International Security*, 2012: 81 - 110.

National Research Council. *At the Nexus of Cybersecurity and Public Policy.* Policy Report, Washington DC: National Research Council, 2014.

—. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press, 1991.

National Science and Technology Council. *Federal Cybersecurity Research and Development Strategic Plan.* Development Plan, Washington, DC: Office of the President, 2016.

Newport, Frank. *Gallup Polling.* January 9, 2007. http://www.gallup.com/poll/26080/public-opposes-troop-surge-61-36-margin.aspx (accessed July 8, 2017).

Nicholson, A., S. Webber, S. Dyer, T. Patel, and H. Janicke. "SCADA Security in the Light of Cyber-Warfare." *Computers and Security*, 2012: 418 - 436.

Nissenbaum, Helen. "Where Computer Security Meets National Security." *Ethics and Information Technology*, 2005: 61 - 73.

NY Times. *One 9/11 Tally: $3.3 Trillion.* September 8, 2011. https://archive.nytimes.com/www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=1 (accessed May 28, 2018).

Nye, Joseph. "Deterrence and Dissuasion in Cyberspace." *International Security*, 2016/2017: 44 - 71.

Nye, Joseph. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly* , 2011: 18 - 38.

Obama, Barack. *Obama White House Archives.* April 1, 2016. https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m (accessed November 24, 2017).

—. "White House Archives." *www.whitehouse.gov.* April 1, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m (accessed November 5, 2017).

Office of the National Counterintelligence Executive. *Foreign Spies Stealing US Economic Secrets in Cyberspace.* Report to Congress on Foreign Economic Collection and Industrial Espionage, Washington, DC: US Congress, 2011.

Orr, Kelly. "Pentagon Computers: How Vulnerable to Spies?" *US News and World Report,* October 31, 1983: 36-37.

Pape, Robert. *Bombing to Win - Airpower and Coercion in War.* Ithaca, NY: Cornell University Press, 1996.

Peterson, Dale. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies,* 2013: 120 - 124.

Poll. "Public Opinion Poll." 60 Minutes / Vanity Fair, January 2010.

Powers, Shawn, and Michael Jablonski. *The Real Cyber War.* Urbana, Chicago, and Springfield: University of Illinois Press, 2015.

President's Commission on Critical Infrastructure Protection. *Critical Foundations - Protecting America's Infrastrctures.* Presidential Report, Washington, DC: White House, 1997.

Quigley, Kevin, Calvin Burns, and Kristen Stallard. "Cyber Gurus: A Rhetorical Analysis of the Language of Cybersecurity Specialists." *Government Information Quarterly,* 2015: 108 - 117.

Rawlinson, Alfred. *The Defence of London, 1915-1918.* London: Melrose, 1923.

Reimer, Jeremy. *Personal Computer Market Share: 1975 - 2004.* http://www.retrocomputing.net/info/siti/total_share.html (accessed October 5, 2018).

Reinhart, RJ. "Cybercrime Tops Americans' Crime Worries." *Gallup.* November 6, 2017. http://news.gallup.com/poll/221270/cybercrime-tops-americans-crime-worries.aspx (accessed May 25, 2018).

Rid, Thomas. *Cyber War Will Not Take Place.* New York, NY: Oxford University Press, 2013 .

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies,* 2012: 5 - 32.

Rid, Thomas. "Cyberwar and Peace: Hacking Can Reduce Real-World Violence." *Foreign Affairs - Council on Foreign Relations*, 2013: 77 - 87.

Rid, Thomas, and Peter McBurney. "Cyber-Weapons." *The RUSI Journal*, 2012: 6 - 13.

Rinear, Matthew. "Armed with a Keyboard: Presidential Directive 20, Cyber-Warfare, and the International Laws of War." *Capital University Law Review*, 2015: 678-720.

Roberts, Lynne, David Indermaur, and Caroline Spiranovic. "Fear of Cyber-Identity Theft and Related Fraudulent Activity." *Psychiatry, Psychology and Law*, 2013: 315 - 328.

Romanosky, Sasha. "Examing the Costs and Causes of Cyber Incidents." *Journal of Cybersecurity*, 2016: 121 - 135.

Roper Center. *iPOLL Search Results.* 2013 - 2016. http://ropercenter.cornell.edu/CFIDE/cf/action/ipoll/ipollResult.cfm?keyword=cyber+attacks&exclude=&topic=Any&organization=Any&fromDate=&toDate=&questionViewId=&label=&studyId=&sortBy=BEG_DATE_DESC&search=submit (accessed November 15, 2016).

Roper Center, Cornell University. *Polling Fundamentals - Total Survey Error.* 2018. https://ropercenter.cornell.edu/support/polling-fundamentals-total-survey-error/ (accessed June 7, 2018).

Sanger, David. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power.* New York: Random House Publishing, 2012.

—. *The Reckoning: How President Obama Has Changed the Force of American Power.* New York: Crown Publishing, 2012.

Schwartau, Winn. *Information Warfare.* New York, NY: Thunder's Mouth Press, 1994.

Seabrook. "Network Insecurity." *The New Yorker*, May 20, 2013: 70.

Shane, Peter. "Cybersecurity Policy as if "Ordinary Citizens" Mattered: The Case for Public Participation in Cyber Policy Making." *Journal of Law and Policy for the Information Society*, 2012: 433 - 462.

Sherry, Michael. *The Rise of American Air Power - The Creation of Armageddon.* New Haven, CT: Yale University Press, 1987.

Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press, 2014.

Smithsonian Air and Space Museum. *300,000 Airplanes.* May 2007. https://www.airspacemag.com/history-of-flight/300000-airplanes-17122703/ (accessed November 2, 2018).

Staff Reporter. "Obama Remarks on Confronting Cyber Terrorist Threats." *Washington Post.* July 16, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/07/16/AR2008071601474.html (accessed November 16, 2016).

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies*, 2013: 101 - 108.

Symantec, Inc. *2015 Security Report.* 2015. https://www.symantec.com/security-center/threat-report (accessed March 30, 2017).

The IEEE Computer Society. "The Morris Worm: A Fifteen-Year Perspective." *IEEE Security and Privacy*, 2003: 35 - 43.

The White House. *Presidential Decision Directive/NSC-63.* PDD, Washington, DC: The White House, 1998.

Timberg, Craig. *In 1998, these hackers said the internet would become a security disaster. Nobody listened.* . June 27, 2015. https://www.dailyherald.com/article/20150627/business/150629234/ (accessed November 15, 2018).

Turak, Natasha. *The Next 9/11 will be a Cyberattack, Security Expert Warns.* June 1, 2018. https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.html (accessed October 14, 2019).

"U.S. Officials Detail Cyber Policy." *Arms Control Today*, 2012: 32-33.

United States Air Force. *AFDD 1, Air Force Basic Doctrine, Organization, and Command.* Pentagon: Department of Defense, 2011.

United States Department of Defense. *The National Military Strategy of the United States.* National Military Strategy, Washington DC: Department of Defense, 2011.

United States Government. *International Strategy for Cyberspace.* International Strategy for Cyberspace, Washington DC: White House, 2011.

United States Government. *National Security Strategy.* NSS, Washington, DC: White House, 2015.

US Army. *Report of the Select Committee of Inquiry into Operations of the United States Air Services.* Congressional Inquiry, Washington, DC: GPO, 1925.

US Congress. "Exploring Common Criteria: Can it Assure that the Federal Government Gets Needed Security in Software?" *Committee on Government Reform.* Washington, DC: US Government Printing Office, 2003. 58.

—. "Hearing Before the Subcommittee on Technology and Competitiveness." *Computer Security.* Washington, DC: US Government Printing Office, 1991.

US Congress. *US Cyber Command: Organizing for Future Operations.* Congressional Hearing, Washington, DC: Government Printing Office, 2010.

US Department of Commerce. *Stolen IP Harms American Businesses.* November 29, 2011. http://2010-2014.commerce.gov/blog/2011/11/29/stolen-intellectual-property-harms-american-businesses-says-acting-deputy-secretary-.html (accessed December 1, 2016).

US Department of Homeland Security. *Homeland Security Presidential Directive 7.* Presidential Directive, Washington, DC: DHS, 2003.

US DOD. *Doctrine of the Armed Forces of the United States.* Joint Publication 1, Pentagon: Department of Defense, 2013.

US General Accounting Office. *Computer Security - Hackers Penetrate DOD Computer Systems.* Congressional Report, Washington, DC: GAO, 1991.

US General Accounting Office. *Computer Security - Virus Highlights Need for Improved Internet Management.* Report to Congress, Washington, DC: US GAO, 1989.

Valeriano, Brandon, and Ryan Maness. *Cyber War Versus Cyber Realities.* New York, NY: Oxford University Press, 2015.

Vohs, Dennish. "THe Financial Executive's Role in Computer Security." *Financial Executive*, April 1981: 30-32.

Watts, James. *Computer Related Fraud Current Issues and Directions.* Speech, Washington, DC: US GAO, 1981.

Weimann, Gabriel. *Terrorism in Cyberspace: The Next Generation.* New York: Columbia University Press, 2015.

Wells, H. G. *The War in the Air.* New York: George Bell and Sons, 1908.

Wendt, Alexander. *Social Theory of International Politics.* Cambridge: Cambridge University Press, 1999.

Westermann, Edward. *Flak: German Anti-Aircraft Defenses, 1914-1945.* Lawrence, KS: University Press of Kansas, 2001.

White House. *Fact Sheet on Presidential Policy Directive 20.* Fact Sheet, Washington DC: White House, 2013.

White House Press Release. *Statement by the President on the Cybersecurity Framework.* Press Release, Washington, DC: White House, 2014.

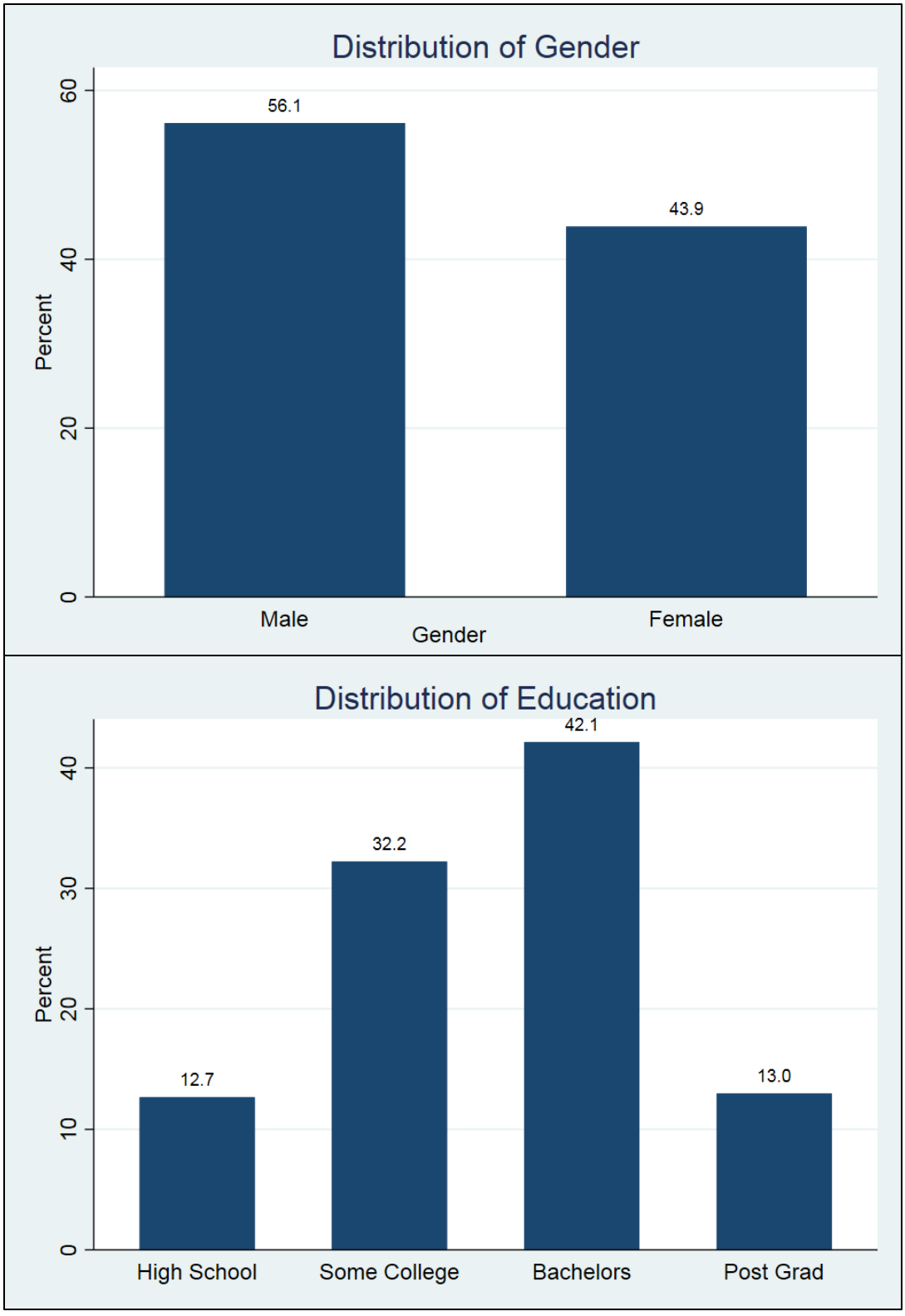
Wilson, Clay. *Information Operations and Cyberwar: Capabilities and Related Policy Issues.* Congressional Report, Washington, DC: Congressional Research Service, 2006.

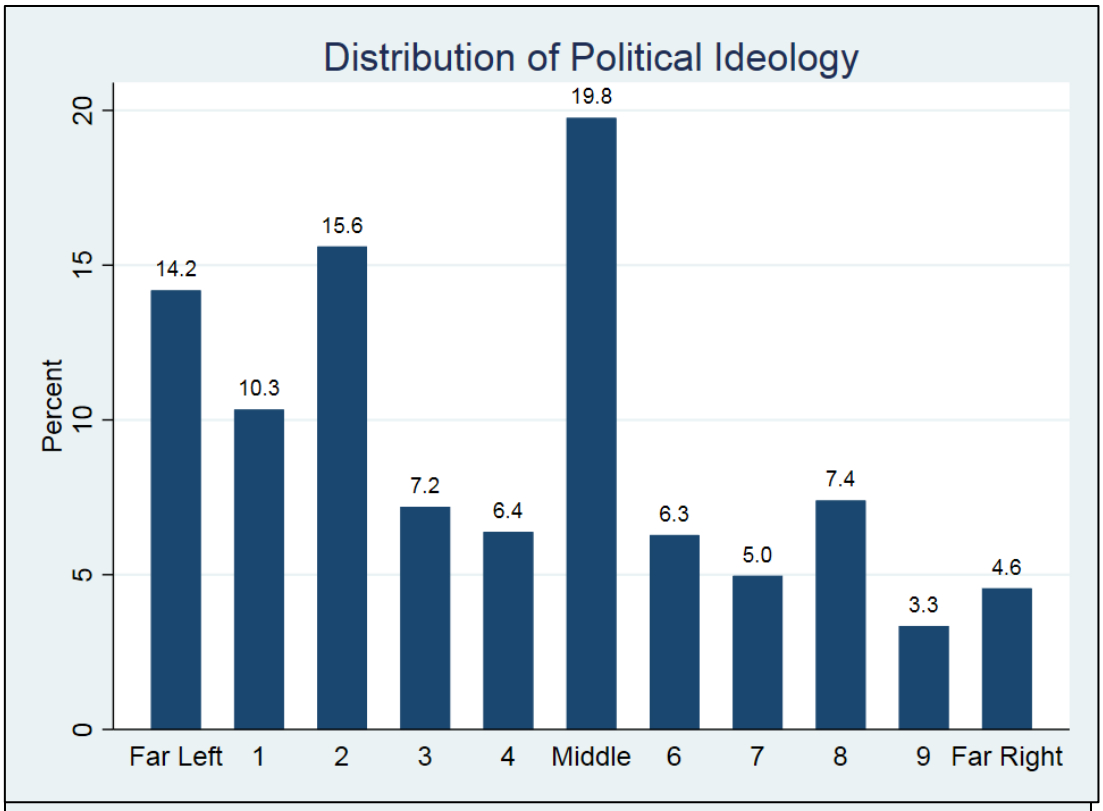
Yannakogeorgos, Panayotis, and Lynn Mattice. *Essential Questions for Cyber Policy.* AFRI Report, Maxwell, AFB: Air University Press, 2011.

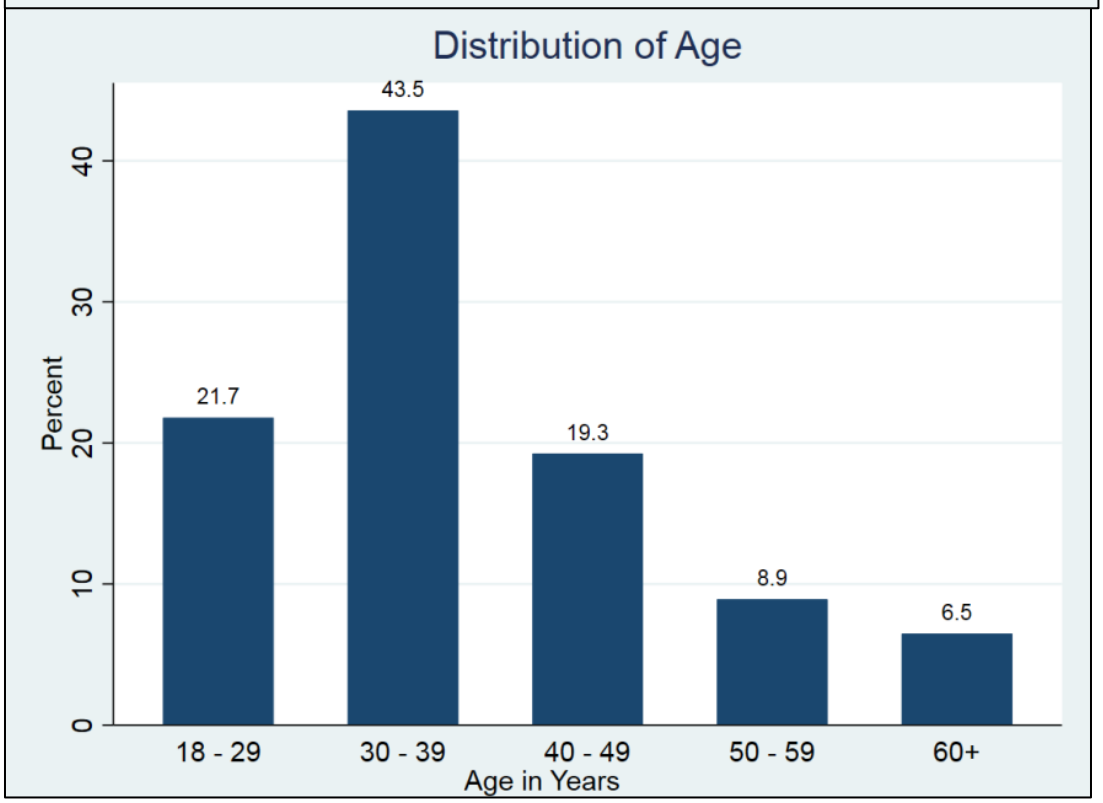
Zheng, Ye. "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond." In *China and Cybersecurity*, by Jon Lindsay, Tai Cheung and Derek Reveron, 123 - 137. New York: Oxford University Press, 2015.

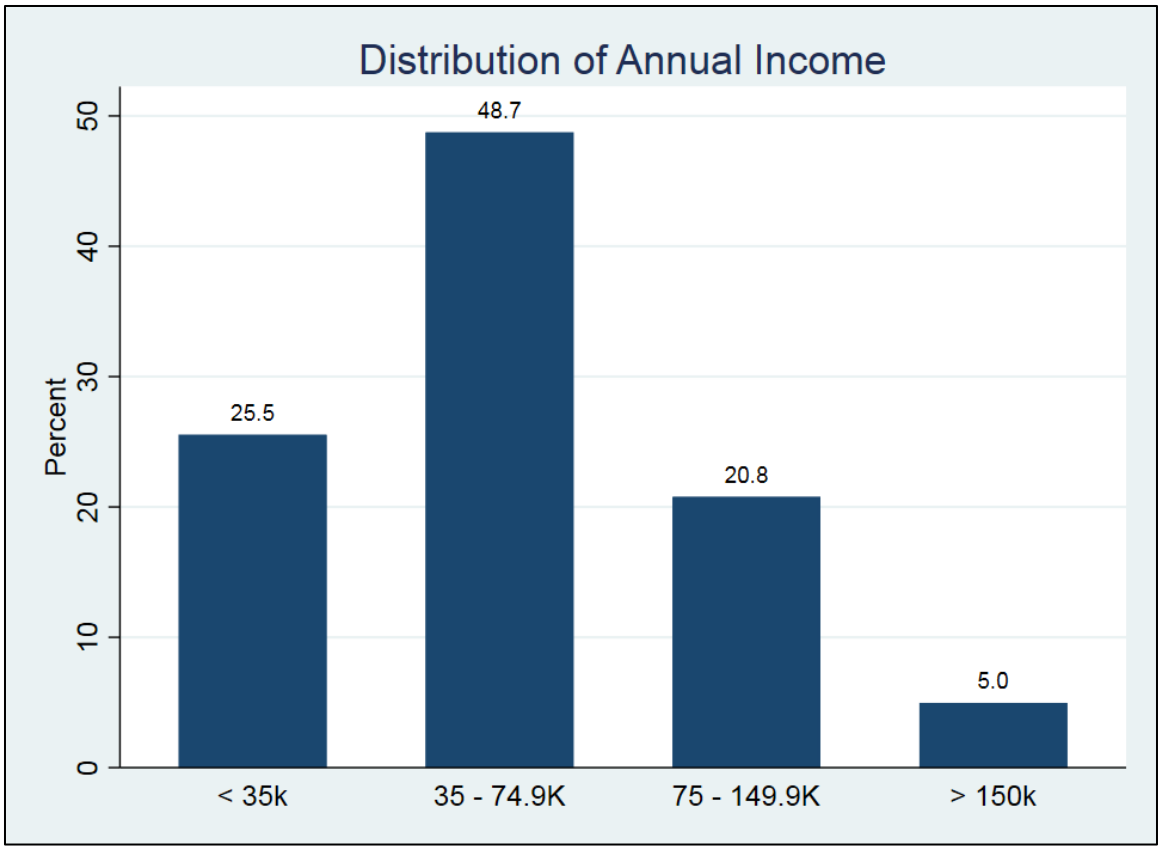
APPENDIX A

Demographics for Public Survey Experiment (n = 987).




Distribution of Political Ideology
Percent
0
5
10
15
20
14.2
10.3
15.6
7.2
6.4
19.8
6.3
5.0
7.4
3.3
4.6
Far Left
1
2
3
4
Middle
6
7
8
9
Far Right

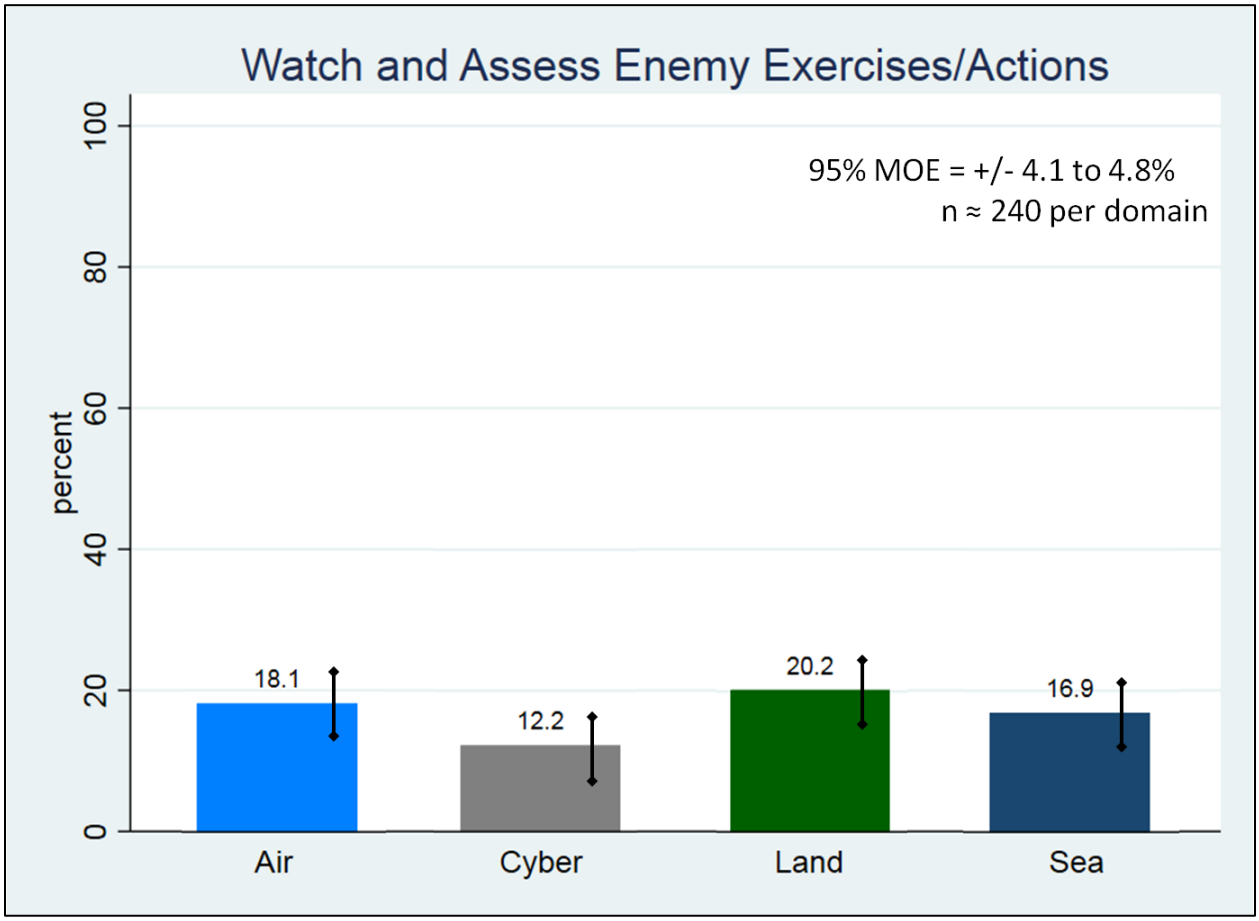

Distribution of Age
Percent
0
10
20
30
40
21.7
43.5
19.3
8.9
6.5
18 - 29
30 - 39
40 - 49
50 - 59
60+
Age in Years


Distribution of Annual Income
Percent
0
10
20
30
40
50
48.7
25.5
20.8
5.0
< 35k
35 - 74.9K
75 - 149.9K
> 150k

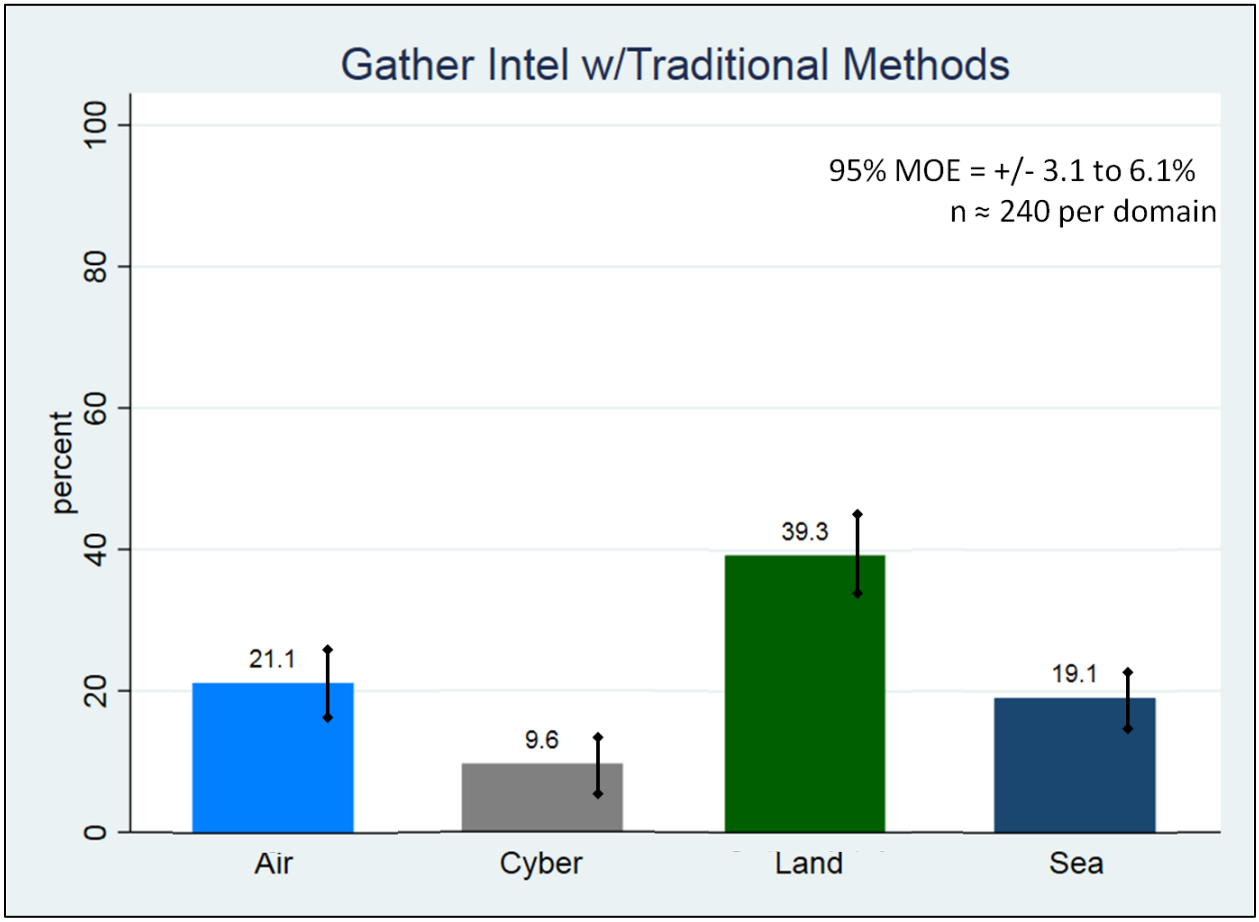
APPENDIX B

Additional Results from H1 Testing.

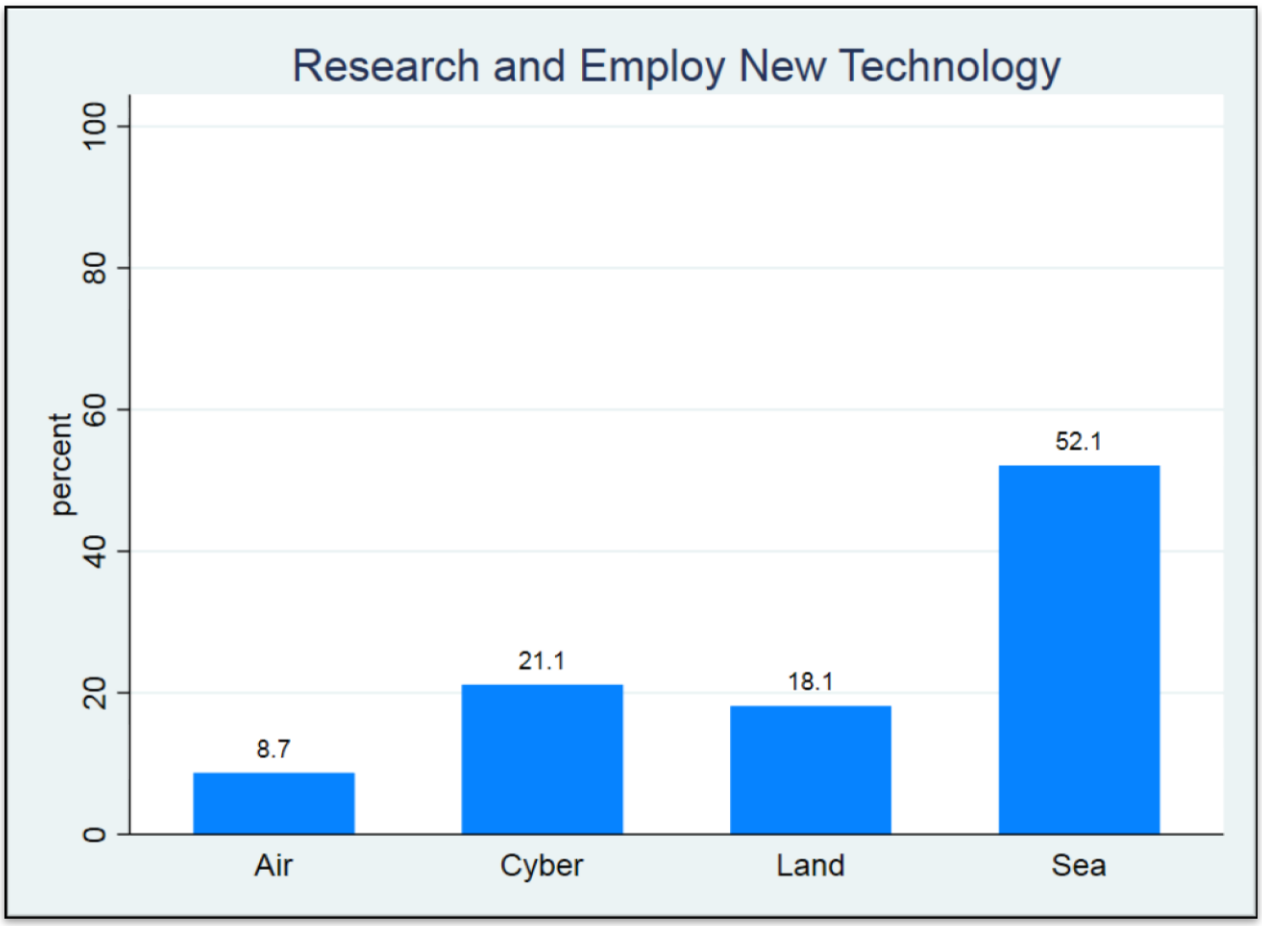
The follow graph shows the results for the watch and assess option from H1. With a 95 percent confidence margin of error of +/- 4.12 percent for each response, there is no statistical difference between domains for the watch and assess option. This and the other following responses are not relevant to the theory; they were simply additional options for respondents to select to provide a balanced set of responses.



The next graph shows the results for the gather intelligence with traditional methods (e.g., spies, informants, etc) option. The land domain received 39.3 percent support, which is statistically significant from the other three domains. The air and sea domain received 21.1 and 19.1 percent, respectively, while the cyber domain placed last with 9.6 percent.



Lastly, this graph shows the results for the last H1 option, which involved researching and employing new technology to strengthen defenses. The sea domain received the most support for this option with 55.4 percent. This is not statistically distinct from the air and cyber domain, which received 52.1 and 44.5 percent respectively. The land domain earned the least support, garnering 34.4 percent of respondent votes.



APPENDIX C

Survey Experiment Questions

Demographic Questions:

D1: Please select your age group:

A. 18-29
B. 30-39
C. 40-49
D. 50-59
E. 60+

D2: Please select your gender:

A. Male
B. Female

D3: Please select your highest level of education:

A. High School
B. Some college, associate degree, or specialized training
C. Undergraduate degree
D. Post postgraduate work or postgraduate degree

D4: What is your total household income from all sources in US dollars?

A. < 30,000
B. 31,000 – 74,000
C. 75,000 – 149,000
D. 150,000 +

D5: In politics, people often talk about the left and the right. Please select your political ideology on a scale of 0 to 10, where 0 is far left, 5 is independent, and 10 is far right:

(Subjects randomized into one of the next four questions)

Q1a: Each day, the US government undertakes numerous actions to strengthen US military air defenses. Which of the following actions do you believe would be most likely to strengthen US military aircraft security in the air domain?

A: Probe enemy air systems with US military aircraft to determine their air capabilities.

B: Gather intelligence through traditional sources (e.g. spies, informants) on enemy air capabilities.

C: Watch and assess enemy military air exercises to determine their air capabilities.

D: Rely on continued evolution of US airpower technology to stay a step ahead of enemy air capabilities.

Q1b: Each day, the US government undertakes numerous actions to strengthen US military cyber defenses. Which of the following actions do you believe would be most likely to strengthen US military security in the cyber domain?

A: Probe enemy cyber networks to determine their cyber capabilities.

B: Gather intelligence through traditional sources (e.g. spies, informants) on enemy cyber capabilities.

C: Watch and assess enemy cyber activity to determine their cyber capabilities.

D: Rely on continued evolution of US cyber technology to stay a step ahead of enemy cyber capabilities.

Q1c: Each day, the US government undertakes numerous actions to strengthen US military naval defenses. Which of the following actions do you believe would be most likely to strengthen US military security in the sea domain?

A: Probe enemy sea defense networks to determine their naval capabilities.

B: Gather intelligence through traditional sources (e.g. spies, informants) on enemy naval capabilities.

C: Watch and assess enemy naval activity to determine their naval capabilities.

D: Rely on continued evolution of US naval technology to stay a step ahead of enemy naval capabilities.

Q1d: Each day, the US government undertakes numerous actions to strengthen US military ground defenses. Which of the following actions do you believe would be most likely to strengthen US military security for ground forces?

A: Have US ground soldiers probe enemy ground defenses to determine their capabilities.

B: Gather intelligence through traditional sources (e.g. spies, informants) on enemy ground capabilities.

C: Watch and assess enemy military ground exercises to determine their ground capabilities.

D: Rely on continue evolution of US land warfare technology to stay a step ahead of enemy ground defenses.

(Subjects randomized into one of the next two questions)

Q2a: Each day, the US government undertakes numerous intelligence gathering operations against adversaries. Each operation entails leaders weighting the risks and benefits of each operation.

- *Today, leaders are assessing whether to undertake a new cyber operation against an enemy military network.*
- *The risk is assessed to be moderate for this particular cyber operation. This means there is a 50/50 chance of gathering the expected intelligence, but also a 50/50 chance of getting caught. Getting caught may cause the enemy to undertake a similar operation against US networks.*
- *If the operation succeeds, it would produce general intelligence that would help US leaders deal with the enemy nation.*

Select your level of support for the operation on a scale from 1 to 10, with 1 being no support, and 10 being full support.

Q2b. Each day, the US government undertakes numerous intelligence gathering operations against adversaries. Each operation entails leaders weighting the risks and benefits of each operation.

- *Today, leaders are assessing whether to undertake a new cyber operation against an enemy military network.*
- *The risk is assessed to be moderate for this particular cyber operation. This means there is a 50/50 chance of gathering the expected intelligence, but also a 50/50 chance of getting caught. Getting caught may cause the enemy to undertake a similar operation against US networks.*
- *If the operation succeeds, it would produce intelligence needed to protect US businesses and military networks against enemy cyber attacks.*

Select your level of support for the operation on a scale from 1 to 10, with 1 being no support, and 10 being full support.

(Subjects randomized into one of the next four questions)

Q3a: Each day, the US government undertakes numerous intelligence gathering operations against adversaries. Recently, the US undertook a cyber operation against an enemy nation to gather intelligence.

- *The operation produced general intelligence that is useful to several US agencies that deal with the enemy nation.*

Based on the information given, would you classify this US cyber operation as offensive or defensive?

Q3b: Each day, the US government undertakes numerous intelligence gathering operations against adversaries. Recently, the US undertook a cyber operation against an enemy nation to gather intelligence.

- *The operation produced cyber intelligence needed to strengthen cyber security for US residents, businesses, and government agencies.*

Based on the information given, would you classify this US cyber operation as offensive or defensive?

Q4a: Each day, enemy nations undertake numerous intelligence gathering operations against the US. Recently, an enemy nation undertook a cyber operation against the US to gather intelligence.

- *US experts believe the enemy operation produced general intelligence that will give the enemy nation an advantage with the US on world issues.*

Based on the information given, would you classify this enemy cyber operation as offensive or defensive?

Q4b: Each day, enemy nations undertake numerous intelligence gathering operations against the US. Recently, an enemy nation undertook a cyber operation against the US to gather intelligence.

- *US experts believe the enemy operation produced cyber intelligence that enemy agencies can use to strengthen their cyber security.*

Based on the information given, would you classify this enemy cyber operation as offensive or defensive?

Q5: Recently, US cyber experts identified two possible national cyber strategies that the US could adopt for the next decade. A common cyber strategy would help US agencies focus on similar cyber objectives and would better align US cyber resources. Please select the cyber strategy that you believe would be most effective for the US over the next decade:

- *Strategy A: Focus on cyber capabilities that can:*
  - *Penetrate nearly any enemy network undetected*
  - *Fight and disrupt enemy military forces without the need for traditional US military forces (e.g. ground soldiers, airplanes, etc)*
  - *Gather nearly any intelligence US leaders need to protect US residents, the economy, and government agencies*
- *Strategy B: Focus on cyber capabilities that can:*
  - *Detect nearly any enemy cyber attack*
  - *Better protect US military forces from disruptive enemy cyber attacks*
  - *Better protect US networks from enemy cyber attacks that could provide intelligence to enemy leaders*

Q6: In the following scenario, I have listed the military budgets for three enemy countries. The enemy countries are identical in all aspects except in their budget for their military cyber forces. With all else being equal, please select the country that you feel presents the <u>LEAST threatening</u> posture to the US:

A: Country A: $9 billion on offensive cyber forces and $1 billion on defensive cyber forces.

B: Country B: $1 billion on offensive cyber forces, and $9 billion on defensive cyber forces.

C: Country C: $5 billion on offensive cyber forces, and $5 billion on defensive cyber forces.

Q7: Suppose US officials recently allocated $10 billion to spend on new US cyber capabilities to take advantage of the opportunities the cyber domain presents. US leaders must decide the percentage of money to allocate to offensive versus defensive cyber capability development. Please use the sliding scale below to indicate the offensive/defensive ratio you believe would give the US the best global advantage over the next decade:

Q8: How often do you, yourself, worry about the following things? (select as few or as many as apply)
Having personal or financial information stolen by computer hackers
Being the victim of identity theft
Having your car stolen or broken into
Your home being burglarized when you are not there
Being the victim of terrorism
Having a school-aged child physically harmed attending school
Getting mugged
Your home being burglarized when you are there
Being the victim of a hate crime
Getting murdered
Being sexually assaulted
Being attacked while you drive your car
Being assaulted/killed by a coworker where you work