

On the Use of Offensive Cyber Capabilities

A Policy Analysis on Offensive US Cyber Policy

By Robert Belk and Matthew Noyes

Advised by Professor Joseph Nye & Professor Monica Toft

20 March 2012

Abstract: Analysis and policy recommendations for use and response to various forms of cyber action for Offensive Military Cyber Policy. Establishes a pragmatic policy-relevant, effects-based ontology for categorizing cyber capabilities. Develops a comprehensive framework for cyber policy analysis. Demonstrates use of the cyber policy analysis framework by analyzing six key categories of external cyber actions identified by our ontology, which range the entire spectrum of cyber activity. Develops actionable policy recommendations from our analysis for cyber policy makers while identifying critical meta-questions.



On the Use of Offensive Cyber Capabilities by Robert Belk and Matthew Noyes is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

About the Authors:

Robert Belk is a Naval aviator and Politico-Military Fellow, studying international and global affairs at the Harvard Kennedy School. In his 16 years of service, he has made four carrier-based deployments and one ground-based deployment to Iraq. Following graduation, he is scheduled to report to the Naval Operations staff in the Pentagon to develop and execute Navy network and cybersecurity policy.

Matthew Noyes studies international security policy and is a senior associate with the cybersecurity practice at Good Harbor Consulting. Prior to attending the Harvard Kennedy School, he served for five years as an infantry officer in the US army serving multiple tours in Iraq. Following graduation he plans to continue working on cybersecurity issues. He has a degree in Computer Science and Applied Computational Mathematics from the University of Washington.

The authors have completed this project to fulfill the capstone Policy Analysis Exercise (PAE) requirement for the Master in Public Policy (MPP) program at the Harvard Kennedy School of Government. All views expressed are our own and do not necessarily reflect the views of the Department of Defense.

Table of Contents

Acknowledgements	3
Executive Summary	4
I. Introduction	8
II. Cyber Policy Ontology	11
III. Framework for Cyber Policy Analysis	27
Normative Considerations	29
Operational Considerations.....	33
Consequential	36
IV. Cyber Actions with Minimal Effect.....	42
Scanning	42
Intrusion	51
V. Non-Disruptive Cyber Actions	65
Data Collection	65
VI. Cyber Attack	75
Cyber Attack	75
Counterattack	91
VII. Cyber Force	111
VIII. Conclusion	129
Appendix 1: Summary of Recommendations	132
Appendix 2: Glossary	139
Bibliography	142

Acknowledgements

This project has dominated much of our time and thought this last year. As such we would like to first thank our friends and family for enduring countless hours of discussion on esoteric cyber policy issues. We have enjoyed the generous support of the ONR research project *Explorations in Cyber International Affairs* at the Harvard Kennedy School for this project; we benefited tremendously from their outstanding work organizing and supporting so many great cyber-policy focused discussions and events at the Kennedy School. Thank you to Eric Rosenbach for pointing us towards such a big “blue ocean” problem. We hope our charting of this fresh intellectual space helps U.S. Defense Policy makers in establishing effective and appropriate policy for the use of external cyber capabilities.

On this voyage we benefited from outstanding advice and guidance from Professors Joseph Nye, Jonathon Zittrain, and Monica Toft; their help was critical as we navigated uncharted waters. We thank all those who took the time to discuss cyber issues with us including Michael Sechrist, Jack Goldsmith, Joel Brenner, Jacob Olcott, Taylor Moore, Herb Lin, GEN Cartwright, Vivek Mohan, Lucas Kello, Jonah Hill, and countless more that visited HKS to speak on cybersecurity issues. A special thanks to Richard Clarke and Eric Rosenbach for getting us started on cybersecurity policy last January and providing us the opportunity to explore challenging cybersecurity issues, first in class at HKS and then at Good Harbor Consulting. Finally, thank you to our readers; we hope this record of our intellectual exploration provides a useful map for your own journeys and we look forward to seeing how you refine our understanding of cyber policy.

Executive Summary

The defining characteristic and critical role of the state is maintaining a monopoly on the legitimate use of force.¹ As time progresses, technological advances change the way individuals and states engage in conflict, and it is incumbent on states to adjust their activities and policies to maintain their control over the use of coercive force. In the Information Age, the Department of Defense (DoD) must develop an understanding of cyberspace and determine its appropriate role in this new domain. In particular, DoD needs to develop an understanding of the policy implications of using offensive cyber capabilities and establish policies for managing their employment. To that aim, we developed the following system for conceptualizing cyberspace and evaluating offensive cyber operations. This system includes two parts: 1) An ontology² for categorizing all operations in cyberspace; and 2) a framework for analyzing the implications of offensive cyber operations. We have analyzed specific key types of offensive cyber operations in order to provide critical policy recommendations, and to demonstrate the application of our cyber policy methodology.

Ontology

Current DoD definitions for Computer Network Operations (CNO) attempt to categorize cyber operations including nebulous definitions of Computer Network Attack (CNA) and Computer Network Defense (CND).³ This intent-based definition is internally inconsistent and fails to provide useful

¹ See (Weber, 1919) and (Hobbes, 1985).

² An ontology is a formal representation of a domain of knowledge as a set of concepts and the relationships between those concepts. An ontology is used to describe and reason within a domain of knowledge.

³ See JP 3-13, (U.S. Joint Chiefs of Staff, 2006).

distinctions for policy-making. To rectify this issue, we have developed the following ontology based on a hierarchy of three criteria.

- 1) Target of the cyber operation: based on ownership of affected networks
- 2) Effect of the operation: by type (logical or physical) and degree (minimal to use of force)
- 3) Objective of the operation: whether informational, offensive or defensive

Using this system, it is clear that current classifications of **offensive cyber operations** are overly broad, applying actually to **external cyber operations**. Given this distinction, we provide a detailed examination of external cyber operations as shown in Figure 1. Within this ontology, we have identified eleven types of external cyber actions, and have conducted detailed analyses of six: 1) Scanning, 2) Intrusion, 3) Information Collection, 4) Cyber Attack, 5) Counterattack, and 6) Cyber Force.

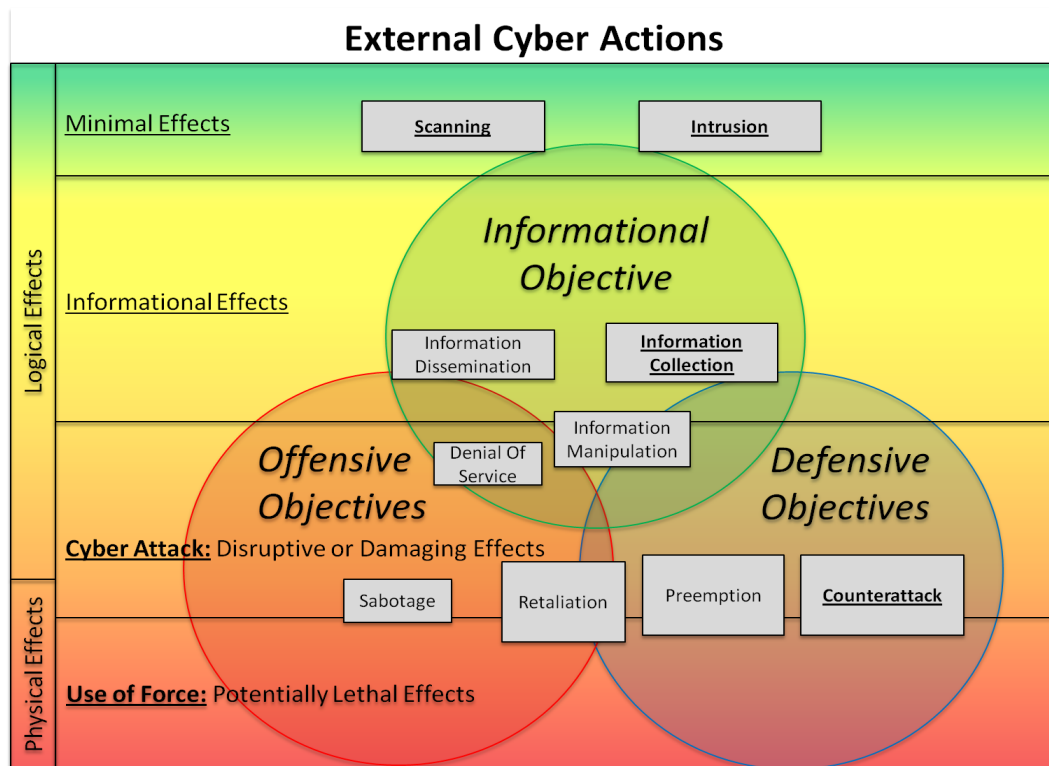


Figure 1: External Cyber Actions Ontology (underlined subject to detailed analysis)

Framework

Assessing the implications for these actions requires a holistic framework that recognizes the potential consequences for conducting external cyber operations. Our framework, shown in Figure 2, contains three aspects and ten considerations. These aspects are weighted from left to right, with Normative aspects being the most significant. Normative considerations include ethical and legal implications of external cyber operations. Operational considerations include the overall strategic and operational implications and could be considered first order effects. Consequential considerations include broader implications for politics, diplomacy and the nature of cyberspace as a medium, and could be considered second and higher order effects.

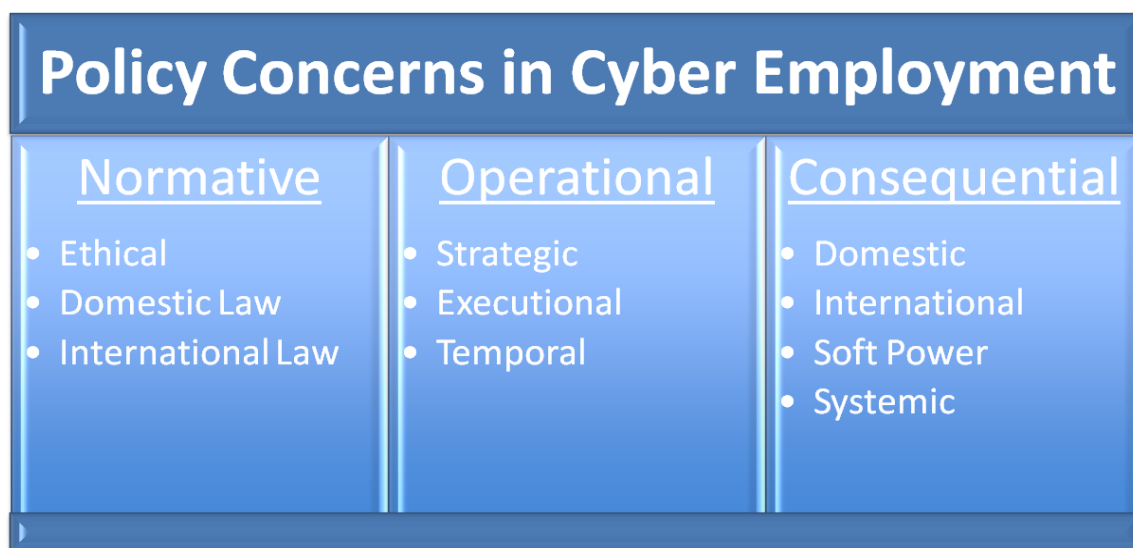


Figure 2: Cyber Policy Analysis Framework

Recommendations

Using this framework, we examined the six external cyber operations identified above. For each of these operations, our analysis yielded general and specific “severity of implication” ratings and policy recommendations for DoD to implement. These recommendations are briefly summarized in Table 1.







Cyber Action	Overall Severity of Implication	Recommendations
Scanning		<ul style="list-style-type: none"> • Establish interagency understanding that scanning is good intelligence practice. • Do not describe scanning as “attacks.” • Conduct with good operational security. • Establish process to share identified vulnerabilities when appropriate.
Intrusion		<ul style="list-style-type: none"> • Conduct only to improve cyberspace security or support higher U.S. strategic objectives. • Establish disclosure procedures for sharing identified vulnerabilities, when appropriate. • Amend the CFAA. • Employ signaling in intrusions when able.
Data Collection		<ul style="list-style-type: none"> • Ensure protection of privacy. • Promote reasonable norms for privacy protection standards. • Continually fund research of new TTPs.
Cyber Attack		<ul style="list-style-type: none"> • Recognize that Cyber Attacks are a useful, short-of-force, tool for political coercion. • Conduct Cyber Attacks only in a manner that is internationally understood to not constitute an “armed attack.”
Counterattack		<ul style="list-style-type: none"> • Develop matrix to categorize counterattack capabilities based on uniqueness. • Create metrics to categorize scenarios based on imperative to act. • Engage in interagency dialogue to create counterattack norms. • Refine method for executing counterattacks. • Create escalation and de-escalation matrix.
Cyber Force		<ul style="list-style-type: none"> • Do not engage in cyber force unless the following conditions are met: <ul style="list-style-type: none"> ○ Conforming to LOAC ○ Minor or no spillover effects (if overt) ○ Coordinated with allied partners and legitimized through multi-national body ○ In concert with traditional military force and as targeted as possible ○ Limit use of catastrophic cyber force to situations of declared general warfare.

Table 1: Summary of Analysis and Recommendations

I. Introduction

Though conflict inevitably occurred previously, the first recorded land war took place in 2700 B.C. between the Sumerians and Elamites (citizens of two city states in modern day Iraq and Iran respectively). Over the next two millennia, the constant presence of warfare in Sumer corresponded with rapid innovations in military technology that outpaced any other location in the world.⁴ In 1210 B.C., King Suppiluliuma II of the Hittite Empire successfully led his naval fleet in battle against the Cypriots. 700 years later the Persian Wars (499 to 449 B.C.) witnessed the first joint land-sea operations.⁵ The first use of aerial technology in combat occurred in China in 202 B.C. during the war of Gaixia between the Chu and Han, during which kites were used most likely for communication purposes.⁶ In essence, mankind has had the luxury of 2200 to 4700 years to understand and refine land, sea and air warfare. Though technology has progressed, from chariots to tanks, triremes to cruisers, and kites to tactical jets, the nature of these battlespaces has not changed.

The same is not the case for cyberspace. In 1981, Apple Viruses 1, 2 and 3 dispersed through Texas A&M through pirated video games.⁷ Initially designed for research purposes, some of the viruses resulted in crashing various programs.⁸ 28 years later, the Stuxnet virus hit the nuclear enrichment facility in Natanz, Iran. Using multiple zero day exploits and vulnerabilities in the SCADA system controlling the centrifuges, the Stuxnet virus destroyed centrifuges and

⁴ (Gabriel & Metz, 1992)

⁵ (Naval Warfare)

⁶ (Global Security)

⁷ (Infoplease)

⁸ (Slade, 1992)

effectively disabled uranium enrichment until it was detected five months later.⁹ In one generation, the “weapons” of cyberspace developed at a pace orders of magnitude faster than for any other battlespace in history.

This evolution also corresponds with a staggering growth in connectivity. In 1981, Arpanet boasted 213 hosts.¹⁰ By 2010, the Internet linked almost 1 billion.¹¹ And although airspace covers the entire globe, even an aircraft using scramjet technology would require over an hour to travel halfway around the world.¹² Network communications, including those required for cyber operations, can make the same trip in under a second.¹³ Not only has the cyber domain expanded at astronomical rates, it has done so while creating a technological framework whose speed has no equivalent in the physical realm.

For many of these reasons, cyber policy is struggling to keep pace. Governments have recognized the potentially significant vulnerabilities in (and opportunities of) cyberspace, and they have rushed to understand the nature of this new, man-made battlespace – a battlespace, one should not forget, that is also a market, a gathering place, a social club, a business tool, and much more. While the particular technology comprising the cyber domain may change, it seems likely that interconnected and interoperable communications technologies will persist and conflicts will take place within this domain for the foreseeable future.

⁹ (Zetter, 2011)

¹⁰ (History of the Internet)

¹¹ (Internet Systems Consortium, 2012)

¹² This figure of course assumes the existence of a tactical scramjet aircraft, instantaneous acceleration to max speed, instantaneous deceleration and no external limitations (such as fuel). For information on scramjet technology, see (Scramjet)

¹³ This figure is derived from the transmission speed of fiber optic cables of approximately 124,000 miles per second.

Unfortunately, we believe that there has still been a lack of clarity in understanding cyberspace. For this reason, we offer the following to address this shortcoming. To do so, we have first created an ontology for cyberspace, a way of thinking about cyber activities. We have also developed a framework for the ontology, that is, a tool to use for developing policy for cyberspace. Lastly, we have applied the framework to various cyber operations in an attempt to demonstrate implications for Department of Defense (DoD) cyber policy. Through this system, we believe that DoD will have a more nuanced and holistic comprehension of cyberspace and the policy options available and their implications.

The Bronze Age lasted 1700 years; the same is true for the Iron Age.¹⁴ The modern era, the Information Age, is developing more rapidly. For this reason it is essential for policy-makers to understand the technology that undergirds this dynamic environment, but in a way that makes recognizes important strategic aspects. These are the motivations behind this work, and we believe that offering this link between technological detail and strategic perspective will enable DoD to make better policy decisions.

¹⁴ (History of the World)

II. Cyber Policy Ontology¹⁵

The majority of current literature on cyber operations suffers from dependence on weak metaphors and unclear or ambiguous definitions. Moreover, to the extent definitions do exist regarding aspects of cyber operations, they are often ill suited for the particular policy debate. This inhibits policy makers from making intelligent decisions and developing effective cyber policy. For this reason, establishing a clear and policy-relevant ontology for cyber operations is the essential first-step for conducting productive cyber policy discussions.

Existing frameworks for cyber operations are typically based on the intent of the cyber action; the popular framework of cyber-crime, cyber-terrorism, hacktivism, and cyber-war is an example of one such intent based methodology. The intent of a cyber action, however, is often unclear or indeterminable. Effective policy must be fundamentally premised upon readily observable attributes. The dependence of existing typological frameworks for cyber on unobservable attributes renders them largely inappropriate for policy discussions.

To correct this flaw we begin our discussion of “offensive cyber” by first presenting an ontology for cyber policy analysis. This ontology provides clear definitions and identifies the pertinent attributes for a discussion of policy for cyber operations. In presenting this ontology, we will first examine the flaws with the existing analytical frameworks and explain the principles behind ours.

¹⁵ An ontology is a formal representation of a domain of knowledge as a set of concepts and the relationships between those concepts. An ontology is used to describe and reason within a domain of knowledge.

To the maximum extent possible we use definitions consistent with Department of Defense Dictionary of Military and Associated Terms (JP 1-2), other DoD literature, and major publications on cyber policy. Yet, because our ontology is predicated on observable attributes, it is inevitable that we depart from some commonly used typological structures.

Flaws with existing analytic frameworks

Current writing on “cybersecurity” lacks a coherent, consistent analytical framework that does more than simply label incidents in cyberspace, but also provides insight into the fundamental characteristics, relationships, and implications of these incidents. The three most common flaws with existing frameworks are:

Absent Distinctions: Many paradigms designed to provide insight into the complexities of cyberspace fail to make relevant distinctions between different cyber activities. The most glaring omission is the lack of separation of “normal” cyber activity from the more “onerous” activities that preoccupy policy makers. What specifically distinguishes the “onerous” from “normal” activity? And more importantly, how does the policy maker provide the cyber warrior with the right distinction? Most systems fail to answer these questions.

Inconsistent Use of Definitions: Though most writings on cybersecurity reference the same historical incidents that drive categorization, the terminology used to examine these events remains fragmented. Different terms are used for the same phenomenon, and the same term is often used to cover disparate phenomena. For instance, effects in cyberspace that do not extend to physical space can be either “non-kinetic” or “logical” depending on the author. Similarly, the meaning of the term “cyber attack” differs

greatly between various sources, and confuses benign cyber activity with hostile action. This lack of consistency obfuscates the more pertinent questions of implications and subsequent policy choices.

Logically Incoherent Analysis: Many works recognize some attributes of a cyber incident are indeterminable, but seek to categorize cyber actions by these attributes. For instance, writings often make the distinction between cyber attacks and cyberexploitation (or cyberespionage) based on intent, yet aver that determining intent in cyberspace is exceptionally difficult or impossible.¹⁶ The consistent failure to address incongruities such as this obscures the conceptualization of cyberspace and undermines the original analysis.

The net result of these shortcomings is a paradigm that is not well suited for policy makers. To illustrate this fact consider the Department of Defense's current definitions for cyber operations as described in Joint Publication 3-13 (Information Operations).

Department of Defense (DoD):

DoD incorporates, and attempts to define, cyberspace operations within the context of information operations. A graphical depiction of this model is shown in Figure 3. DoD labels

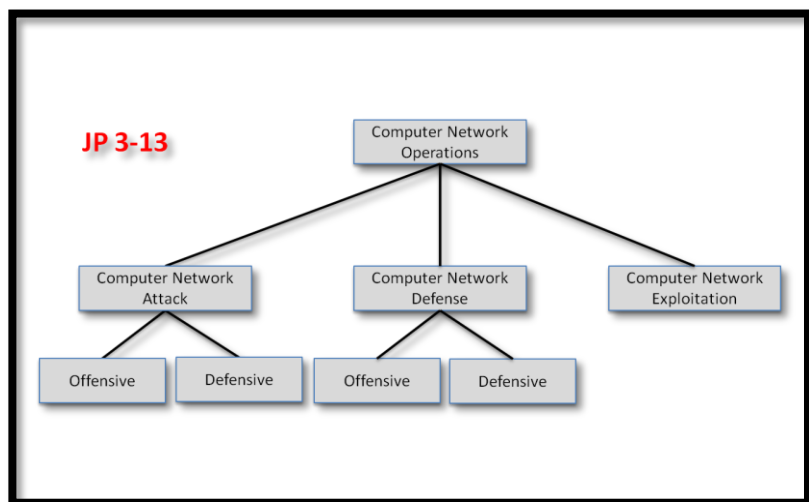


Figure 3: DoD Cyber Framework

¹⁶ See for example US CERT, Cyber Threat Source Descriptions, (US-CERT)

these cyberspace operations “computer network operations” (CNO), yet provides no distinction between CNO and any other type of computer network activity. Instead, DoD defines CNO simply as “Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.”¹⁷ This definition, though consistent with the framework, does not illuminate the key elements of CNO, nor does it differentiate CNO from other activity in cyberspace.

As a subset of CNO, “computer network attack” (CNA) is defined as “[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA.”¹⁸ In contrast, DoD defines “computer network defense” (CND) as “[a]ctions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity with Department of Defense information systems and computer networks. Also called CND.”¹⁹ These definitions themselves are somewhat problematic, because in essence they are not describing the activities within cyberspace, but rather the nature of “offense” and “defense.” In cyberspace, however, acting offensively or defensively is not as distinct as in physical space.²⁰

JP 3-13 further muddies the picture by stating, “All IO capabilities may be employed in both offensive and defensive operations.” According to this claim,

¹⁷ (U.S. Joint Chiefs of Staff, 2006).

¹⁸ (U.S. Joint Chiefs of Staff, 2006)

¹⁹ (U.S. Joint Chiefs of Staff, 2006)

²⁰ A useful example here, which will also demonstrate the basis of our distinctions, is the difference between offensive counter air (OCA) and defensive counter air (DCA). Both utilize the same weapons and share many of the same tactics, yet OCA aircraft operate over hostile territory while DCA aircraft are protecting either neutral or friendly territory (or a friendly asset). In cyberspace, defensive operations are not limited to one’s own “territory”.

there are offensive and defensive CNA and offensive and defensive CND. In its examination of “offensive cyber”, the National Research Council of the National Academies (hereafter, NRC) recognized this distinction and offered an illustrative example: “[U]nder this rubric, a computer network attack might be used for a defensive purpose, such as the neutralization of a cyberthreat to a DOD computer or network.”²¹ If the NRC’s example accurately represents DoD’s intent in JP 3-13, then this hypothetical overlaps the definition of CND, because it would be an action taken through the use of computer networks to protect DoD networks.

NRC does not offer an example in which a computer network defense might be used for offensive purposes. Either such a case would look very much like the CNA for defensive purposes example or it would be an illogical one. Though we acknowledge that there is a category of cyber operation that is essentially a counterattack (a defensive measure), it is only defined in part by intent. Attempting to define it otherwise produces an illogical framework.

Yet most importantly for this paper, the DoD framework does not provide relevant distinctions that address policy considerations. Specifically, is there something in the nature of CND that enables more permissive conditions for its use relative to the nature of CNA? If that were the case, then a convenient loophole would seem to exist that would permit commanders to label all CNA as actually offensive CND. These definitions, therefore, do not distinguish between the different operations in cyberspace in a manner that establishes the nature of their key differences. This prevents policy makers from having fruitful discussions or establishing effective policies.

²¹ See section 3.1 of (National Research Council, 2009)

Principles Driving the Ontological Framework

In order to rectify this issue, we have developed an ontology that establishes a rational basis for strategic cyber analysis, and a common terminology for establishing cyber policy and doctrine. Our ontology follows naturally from a set of principles derived from the fundamental aspects of cyberspace.

Anonymity: Modern communications protocols emphasize facility of communication and have minimal measures to credibly ensure identification. This fact has resulted in the ability of cyber actors to engage in conduct with substantial anonymity. Though clandestine and covert operations occur in the physical world, there is no physical analogue for the widespread challenge of credibly connecting observed events with an identifiable actor which exists in cyberspace. This nuanced problem of attribution has been explored by a number of scholars.²²

Speed: Most communications over cyber networks occur in milliseconds. This permits actors to engage in conflict at unprecedented speed while being separated by tens of thousands of miles and produce effects that spread quickly to affect users around the globe. Not even nuclear warfare using ICBMs matches the ubiquitous, rapid and global engagements possible in cyberspace.

Borderless: Due to widespread interoperability and interconnection, there are essentially no formal boundaries in cyberspace. Connecting to a server in a foreign nation requires no visa or passport. Though the Westphalian concept of nation state boundaries in the physical world has arguably diminished

²² One excellent example is Clark and Landau, “Untangling Attribution”. See (National Research Council, 2010).

somewhat with globalization, it is far from obsolete as governments continue to apply physical coercion to have some measure of control.²³ Still, there is no analogue in the physical world for the ease of movement in cyberspace and the ability to induce effects across national borders. Moreover, when the actors are beyond the reach of government coercion, either because of size or anonymity, cyberspace is witnessed in its most borderless manifestation.

Ontology for Cyber Policy Making

The following definitions begin at the macro level and narrow in focus. This project centers on cyber operations affecting systems not owned or operated by the actor, and we developed this ontology accordingly. Specifically, we identify, but do not establish in depth, a conceptual category for normal or routine cyber activities. We have focused on fleshing out the nuances of external cyber operations, the characteristics that separate them from other activities in cyberspace, and the relevant attributes that should drive policy analysis. In doing so we introduce a number of terms, identify key attributes for analysis, and illustrate conceptual inter-relationships.

Cyber activity is all activity conducted through *cyberspace*. We define *cyberspace* similarly to JP 1-2 as “a global domain consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”²⁴ What is possible in cyberspace is determined by the “laws of code,”²⁵ as described by Lawrence Lessig, and is continually evolving and changing.

²³ (Goldsmith & Wu, 2007)

²⁴ (U.S. Joint Chiefs of Staff, 2012)

²⁵ (Lessig, 1999)

Cyber activity can have both *logical* and *physical effects*.²⁶ *Logical effects* are those effects contained within cyberspace with minimal (beyond changes to the physical storage media) physically observable manifestations. All cyber activity has logical effects. *Physical effects* are those effects that are physically observable by people; only some cyber operations have physical effects, for example manipulating industrial control systems to produce mechanical failures.

Cyber activity is limited to that which is conducted through cyberspace. We are explicitly excluding from the definition of cyber activity those actions that affect cyberspace but are conducted in the physical domain (free from the laws of the code), such as cutting communication cables or jamming radio frequencies. Actions in the physical domain affecting communications systems are a long standing aspect of warfare with established policy understanding. For analytical clarity this project focuses on just those actions conducted through cyberspace.

Cyber action is the subset of cyber activity that includes interaction with cyber systems that produce effects beyond that which is generally found during normal operation. This set of cyber action explicitly excludes all ordinary or intended uses of cyberspace occurring in accordance with authorized permission or access levels or those actions that do not produce a significant effect. Cyber action is the relevant domain of analysis for this project, and we do not provide further analysis of the broader set of cyber activity that produces no significant effect or is benign in nature.

There are two principal readily observable categories of cyber actions: *external actions* and *internal actions*. We define *external cyber actions* as those cyber actions with effects on systems not owned or operated by the actor.

²⁶ (See Rattray and Healy, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use", National Research Council, *supra* note 21, 77-97)

Internal cyber actions are defined similarly as actions with effects only on systems owned or operated by the actor. Scanning ports of an adversary's system in order to find vulnerabilities is an example of an external cyber action. Scanning ports on one's own system in order to identify flaws in the network is an example of an internal cyber action. This apparently simple and basic distinction is actually the source of much confusion in some policy debates. What we have defined as external cyber operations is often referred to as an "offensive cyber attack," which is a poor description of the action from a DoD policy perspective, obscuring it with military definitions of attack and offense. From a security policy perspective, internal actions (those that only affect one's own systems) do not pose relevant concerns in discussion of national security or international relations. External actions, however, do require analysis and justification, and are the focus of this project.

Many external cyber actions, particularly those attempting to acquire information, are executed through achieving unauthorized access to a computer system, or an intrusion. For many cyber actions an attempted or successful intrusion is the first observable event. Attempted intrusions are often erroneously reported as "cyber attacks." This greatly exaggerates the threat and leads to astronomical threat reports. For example Senator Susan Collins wrote: "Every month, an estimated 1.8 billion cyberattacks target the computer systems of Congress and executive branch agencies, according to the Senate's sergeant at arms."²⁷ Senator Collins is actually referring to the suspected number of attempted intrusions (via scanning or other methods) and not actual cyber attacks. This type of alarmist hyperbole erodes the nuance that exists in

²⁷ (Collins, 2011)

cyberspace and complicates sound national security policy making.²⁸ Given that intrusions or attempted intrusions are often the first observable event, we address intrusions directly and make policy recommendations for reacting to and conducting cyber intrusions.

Some, but not all, cyber actions are directed towards accomplishing strategic objectives; these actions are *cyber operations*. We follow the JP 1-2 definition of objective as *"The clearly defined, decisive, and attainable goal toward which every operation is directed."* Cyber operations pose a much graver security dilemma than mere actions, because they indicate a sustained and dedicated campaign and the presence of an organized adversary. Thus, policy for engaging in, or responding to, cyber operations must be different than engaging in or responding to mere cyber actions.

Determining that a particular observed cyber action is part of a cyber operation can be difficult, but can still be achieved through examining the characteristics of various cyber actions to determine whether they are a part of a sustained campaign or not. Identifying a cyber operation is simpler than divining intent, because it only requires determining that there exists a goal and a dedicated campaign to achieve it. It does not require determining what that goal is or who is attempting to achieve it. Advanced Persistent Threats (APTs)²⁹ are one common example of observed actors engaging in cyber operations. Their activities are typically identified as operations before the precise intent of the operation is determined.

²⁸ (Brito & Watkins, 2012)

²⁹ An APT is an organization with the capability and the intent to persistently and effectively conduct offensive cyber operations against a specific targeted organization.

The objective of an operation can be offensive, defensive, or informational in nature. *Offensive objectives* are those seeking to coerce rival action, impose harm, or degrade rival capabilities. *Defensive objectives* are those seeking to secure one's own systems, and preserve freedom of operation. *Informational objectives* seek either to access or to expose information that is not generally, or publically, available. There exists some overlap between these three categories. For example, one may degrade rival capabilities as part of a counter-attack, giving an operation both an offensive and defensive characteristic. However, these categories are still useful for characterizing external cyber operations based on the nature of the objectives sought.

Determining which of the three categories the objective of an observed cyber operation fits into requires significant analysis to further define intent and may not be readily apparent. However, we believe that it is often possible to determine the type of objectives a cyber operation is pursuing through its effects and design, and policy responses can be tailored accordingly. Offensive external cyber operations pose the most severe policy problems, but defensive external cyber operations, such as counter-attacks, also require the attention of policy makers, and may be an area for early progress in international cyber norm setting and policy making.

Categorizing Cyber

Recognizing that external cyber action is the area of most significant concern for national security policy due to their effect on outside systems, we developed the following ontology (Figure 4) to subdivide the set of external cyber actions for further analysis based principally on effects in ascending order of minimal/no effect, informational effects, disruptive or damaging effects, and effects rising equivalent to a use of force in international law. We do not intend the identified categories as an exhaustive or complete typology of external

cyber action, but we do find them to be the most critical categories for the current policy debate. As such, we subject each of the below categories to further policy analysis along with illustrative case studies in the subsequent sections.

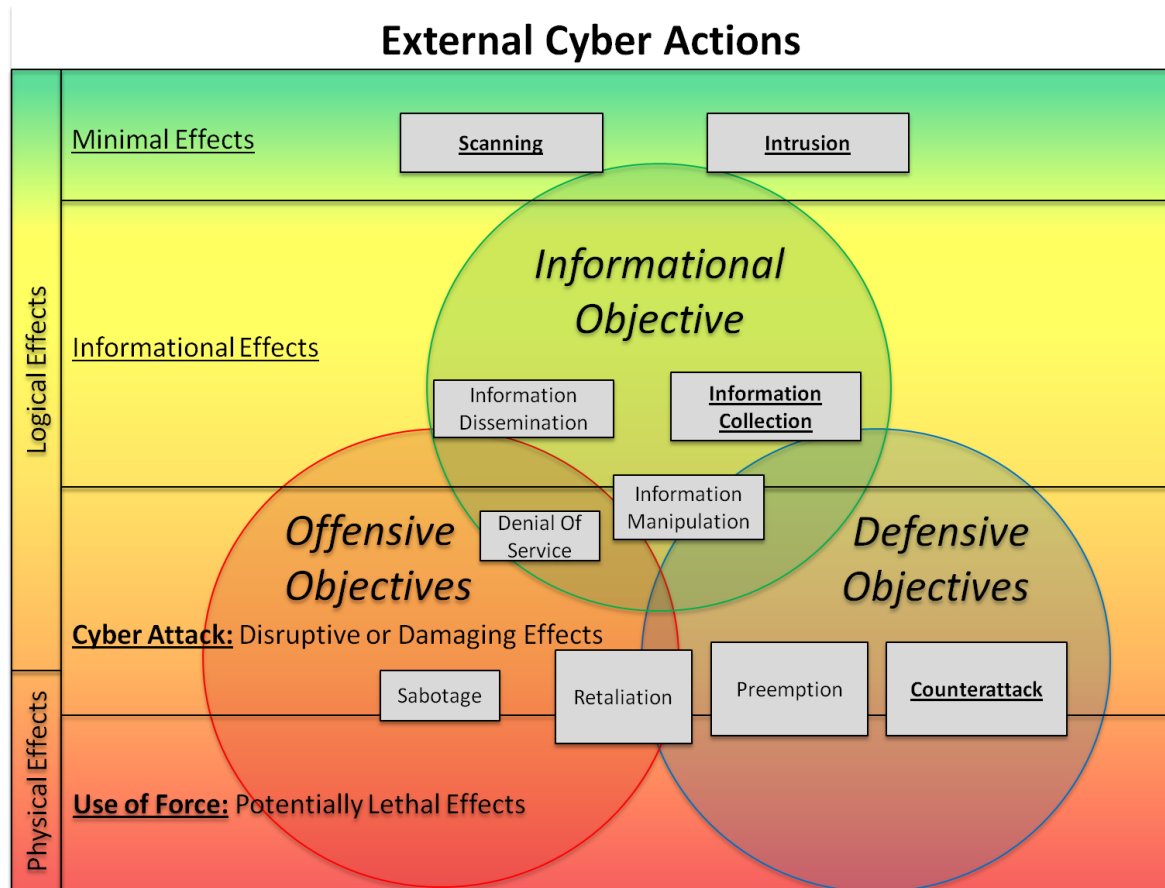


Figure 4: External Cyber Action Ontology

Minimal/No Effect

Cyber Scanning: The conducting of scans to look for potential vulnerabilities. This is actually best considered a cyber activity, not an action; however, scanning is often the subject of excess concern and threat exaggeration so we address it directly.

Cyber Intrusion: Unauthorized access of a computer system. An attempted cyber intrusion is often the first observable action of a cyber operation.

Informational Effects, not disruptive or damaging

Cyber Information Collection: External cyber actions that have no substantial disruptive or destructive effect, but access protected information. Protected information is all information not authorized for general access and normally unavailable to the accessing party.

Cyber Information Dissemination: External cyber actions that have no substantial direct disruptive or destructive effect, but which disseminate protected information to a non-privileged audience. For example, Wikileaks publically posting classified documents. Such operations are inherently offensive in nature.

Disruptive or Damaging Effects

Cyber Attack: External cyber actions with disruptive or damaging logical or physical effects. Cyber attacks can support offensive, defensive, or informational objectives.

This category poses the most challenging policy issues, because cyber attacks in this category exist in a space below violence yet above espionage. For this reason, analogies to either armed conflict or intelligence activities are inappropriate. A detailed analysis of this category requires consideration of intent, circumstances, and precise effects to establish sub-categories of cyber attack. We devote special focus to analyzing the policy for defensive cyber counterattack, which is the most permissible, from a policy perspective, of any form of cyber attack.

Cyber Counterattack: External cyber operations to stop an ongoing use of offensive cyber action. For example, by stopping an ongoing DDOS attack by affecting the participating computer systems.

Cyber Pre-emption: External cyber operation to prevent an anticipated use of offensive cyber action. For example, by conducting taking down a botnet that will eventually be used to conduct an offensive cyber action.

Cyber Retaliation: External cyber operation to impose costs on an actor for aggressive actions. Cyber Retaliation could be a tool to establish deterrence in international relations short of using force.

Denial of Service: Disrupting access to information services without disrupting the confidentiality or integrity of the data, or destroying any systems. Such attacks are commonly conducted by botnets in a distributed denial of service attack (DDoS).

Cyber Sabotage: Cyber attacks which cause the physical destruction of equipment or systems, without directly endangering human life, typically accomplished through giving improper commands to industrial control systems. Stuxnet was a cyber sabotage attack.

Most Severe Effects

Cyber Force: Cyber attacks are attacks with such substantial physical effects that they rise to a level that ought to be considered a “use of force” or “armed attack” under international law. Because Cyber Force requires substantial physical effects, it must support either offensive or defensive objectives. Purely informational effects (even destruction or altering of information) are only logical effects and likely would not rise to the level of a “use of force” under international law. We separate this sub-category out from cyber attacks because of its special policy implications.

Deterrence and Defense

*"To the issue of where we're going in the future and deterrence-type strategies associated with cyber and then how they're incorporated into larger deterrence strategies, today we have a network that is essentially constructed around point defenses. In other words, you go buy a firewall and some sort of virus protection, you put it on your computer. That's a point defense. It tends to be the most inefficient defense there is, because you're static; in any attack on you, you're just always there. [As an Attacker] you just keep [attacking] as often as you want, and there's really no penalty for doing it."*³⁰ -General James Cartwright

One final area worth clarifying is the difference between deterrence and defense. Substantial ambiguity and confusion exists in the current literature on the relationship between deterrence and defense.³¹ It is essential that this distinction is clear in order to have a productive policy discussion. In this work, we follow the definition of deterrence found in JP 1-2 of *"the prevention of action by the existence of a credible threat of unacceptable counteraction."* This we term active deterrence.

Defense protects systems, directly increasing the *cost to conduct* a successful attack. Deterrence increases the *cost should an attack succeed either through* threatened retaliatory action or entanglement (passive deterrence). Given the valuable information stored in cyberspace and the high cost of defending this information, we agree with the analysis of retired General Cartwright³² that organizations which only defend and do not deter against cyber attacks are certain to be the victims of cyber attacks as long as they use information systems.

All deterrence is inherently achieved through creating a system where adversaries believe that a successful attack will impose additional costs on them that exceed the benefits of an attack. This is generally achieved through

³⁰ (Lynn & Cartwright, 2011)

³¹ For example, see (Gourley, 2008)

³² (Nakashima, 2011)

threatening external action or entanglement, respectfully described as active and passive deterrence. Active deterrence is often achieved through threatened legal or law enforcement activity, but for actors beyond the reach of law, active deterrence is achieved through threatened military or other state action. As a part of this work we will be exploring what sorts of external cyber action could and should be employed to achieve an active deterrent effect while following, where applicable, the principles of the law of armed conflict such as military necessity, proportionality, and distinction. Active deterrence strategies are most credible when officially declared in policy along with a clear demonstration of capability, but any declared policy will have a norm setting effect in the international community. As such we explore what sorts of cyber deterrence policies, and use of offensive cyber action, that the U.S. should be willing to accept as a new norm for behavior in cyberspace.

Conclusion

The above ontology provides policy makers a system that recognizes the defining characteristics of the Internet and provides a consistent means for categorizing the relevant activities within it. It moves away from an intent-based typology and instead focuses primarily on the effects and ownership of the affected system. This provides greater clarity to policy makers who analyze cybersecurity policy in order to support national security objectives.

Sections IV-VII will examine the cyber policy implications of the key categories defined by this ontology and the effect that various considerations have on policy development regarding the areas we have outlined. Additionally we will provide plausible scenarios to illustrate the above types of external cyber operations and recommendations for legitimate, legal and effective external cyber actions.

III. Framework for Cyber Policy Analysis

In order to provide policy recommendations for external cyber operations, it is important to define the framework through which we derive these recommendations. Though some have attempted to analyze cyber operations through the lens of nuclear deterrence³³ or even as a direct analogue of operations in other domains,³⁴ we believe that such systems fail to capture the myriad of relevant considerations that are particular to cyber operations.

To correct this shortcoming, we have developed a framework that elucidates the critical considerations for employing external cyber capabilities, and therefore the policy for external cyber capability use. In creating this framework, we recognize that the viability of many of the cyber activities we have defined is often context dependent. Though it would be convenient to have clearly defined rules of engagement for cyber policy,³⁵ this is an ambitious goal given the current nature of cyberspace.³⁶ For this reason, our framework is not a checklist that provides a quantitative output, but rather a conceptual mechanism to gauge external cyber operations.

Our framework includes three aspects, which, in order of significance, are Normative, Operational, and Consequential. (See Figure 5.) Within these three aspects we have identified a total of 10 critical considerations. These are also listed in order of significance. This approach provides a holistic and sound model for considering cyber policy implications. Because the validity of cyber

³³ (McConnell, 2010)

³⁴ (Williams, 2011)

³⁵ For a generally recent example of a push for defined rules of engagement in cyberspace, *see* Shanker, 2011.

³⁶ (Greenemeier, 2011)

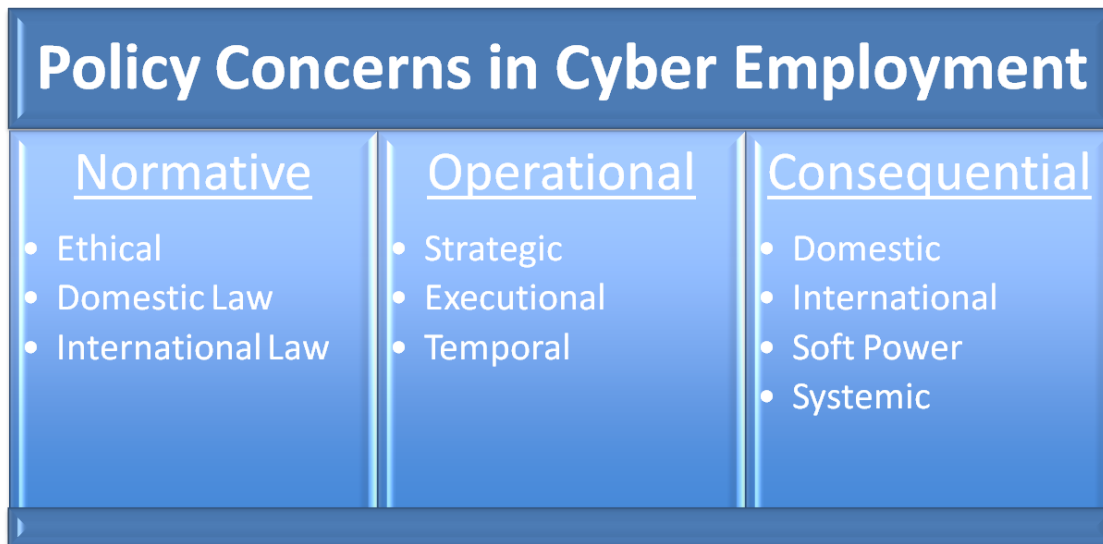


Figure 5: Framework for Cyber Policy Analysis

operations is often context dependent, it is not necessarily intended for policy-makers to use this framework in a linear fashion. In conceptualizing our recommendations, however, it is useful to proceed sequentially through the aspects and considerations.

First, consider the normative permissibility of the action. What are the key constraints dictating the permissibility of the action? For instance, it is not enough to determine whether the action is permissible under domestic and international law; we must consider whether the action is ethically permissible and in accordance with American values. Additionally, do laws need to be adjusted to better align with what is ethically right and best for society?

Next consider the direct operational impacts of the action. Will the action support National Security Strategy? Can the effects be discriminate, controlled, proportional and timely? In short, can the action reliably and effectively achieve the desired effects?

Finally, consider the consequences of the external cyber action. What are the second, third, and higher order effects? Such effects include the domestic reaction, the international state reaction and the effects on American soft power.

Additionally, how might the nature of cyberspace adapt or change in response to the use of a particular cyber action?

Considering all three sets of cyber policy considerations is critical to formulating sound cyber policy, and we will discuss each consideration in detail in order to better understand the challenges for external cyber operations.

Normative Considerations

Ethical

It is not our intention to justify a particular ethical framework by which we will gauge the morality of any external cyber activity. Rather it is important to note that there is a moral dimension to external cyber activity that may not be captured by simply analyzing the legal implications of said activity. By way of an analogy, the U.S. decision to categorize “enhanced interrogation techniques” as legal³⁷ reflected a certain regard for the need for legal justification. It did not, however, reflect on the moral dimension of these techniques. Put another way, simply because we determine that an action is legal, it does not make it morally acceptable.

In that regard, we believe that there are certain ethical aspects that are particularly germane here. First is the applicability of contractualist thought,³⁸ regardless of the international characteristic of external cyber operations. It is not necessary to adhere to a more cosmopolitan view for this belief to hold. At a minimum, however, cyber policy should recognize the potential for unforeseen

³⁷ For a synopsis of the relevant documents, see (Torture Memos).

³⁸ By “contractualist thought” we are referring to John Rawls’s *Theory of Justice*. We are well aware that Rawls did not believe his theory applied internationally, but it is not the complete theory we are advocating either. Rather, we are simply averring that there exists, at a minimum, a basic regard that we extend to human beings that is not particularly captured in consequentialist thought.

effects of external cyber operations that may affect civilians. Just as different ROE criteria require different collateral damage estimates (CDE) for conventional weapons, different scenarios in cyberspace will often require varying degrees of protection against collateral damage.

Another ethical aspect we must consider is the quintessential American values of wariness of government, and the high value placed on democratic openness and freedom of expression. The majority of actions in cyberspace consist primarily of informational effects, and the U.S. must ensure any cyber actions taken do not significantly reduce people's legitimate freedom to share information. To act in a manner contradictory to this ethic may erode America's moral legitimacy and soft power in the world.

Thus, we must justify our external cyber operations in a manner that extends beyond meeting the requirements of established laws and rules; we must determine whether or not the operation or policy is ethically permissible.

Legal

It is self-evident that in a nation governed by the rule of law legal considerations play a critical role in policy development. This is particularly true – though perhaps more problematic – in the case of cyber activity. Though cyber activity is a relatively recent phenomenon, there have been some in-depth analyses of the legal implications of external cyber operations.³⁹ We are not qualified to offer legal opinions, but we will highlight some of these arguments in the policy recommendation section that follows. Here, however, we will detail some of the domestic and international legal considerations that impact policy-making in cybersecurity.

³⁹ For examples see (Schmitt, 1999), (Roscini, 2010), (Bradbury, 2011)

Domestic Law

The domestic legal environment is particularly complex for cyber operations. Principally, the 4th amendment to the U.S. Constitution offers protection against unreasonable searches and seizures. This has significant implications for international cyber operations against the U.S. that have a domestic nexus (e.g. a foreign-operated botnet that employs thousands of U.S. computers). Though not specifically codified in the U.S. Constitution,⁴⁰ the established right to privacy plays another role in this same vein. Additionally, the Foreign Intelligence Surveillance Act (FISA) (as modified in 2008) protects citizens at home or abroad from electronic government surveillance without a warrant from a FISA court. This may hinder, for instance, the ability of government agencies to monitor Internet traffic of a U.S. citizen even if that individual's computer or network is linked to (or has been coopted by) a foreign cyber actor.

Legislation like the Computer Fraud and Abuse Act (CFAA) and the Digital Millennium Copyright Act (DMCA) place further constraints on what sorts of cyber activity is legal. Lastly, the United States Code Titles 10 and 50 delineate the authorities, responsibilities and limitations for the Intelligence Community (IC) and the Department of Defense respectively. Because the IC and DoD often overlap with regard to cyber actions, this poses another complicating factor for cyber policy makers.

⁴⁰ For a brief synopsis, *see* (Linder, 2012)

International Law

International considerations may be even more complex. Primarily, the treaties and customary laws that constitute the Law of Armed Conflict (LOAC)⁴¹, including *jus ad bellum* and *jus in bello* tenets, play a key role in military policy. The main principles of distinction, proportionality and necessity are not only guiding tenets, but also exceptionally problematic in the realm of cyberspace.

Multilateral treaties and agreements, such as the 2001 Budapest Convention on Cybercrime delineates five criminal offenses with respect to cyber activity, which countries have implemented through various domestic legislation.⁴² Navigating the variety of international cyber law, of highly variable sophistication, and working towards a normalized transnational cyber law regime will be a persistent challenge in cyber policy for the foreseeable future.

The U.N. charter offers guidelines for the conduct between nations regarding the use of force (in Article 2 (4))⁴³ and self-defense (in Article 51).⁴⁴ Specific case law exists as well that has relevance to policy for external cyber operations.⁴⁵ The Universal Declaration of Human Rights Article 19 provides further protections to individuals' freedom to "seek, receive and impart information and ideas through any media and regardless of frontiers."⁴⁶ Respecting this human right and balancing it with conflicting human rights (such as the right to life, privacy, and property) is one of the core challenges in cyber policy formation.

⁴¹ (International Humanitarian Law Research, 2009)

⁴² (Council of Europe, 2001)

⁴³ (United Nations, 1945)

⁴⁴ (United Nations, 1945)

⁴⁵ Of note are rulings by the International Court of Justice regarding Nicaragua (Nicaragua v. United States of America, 1986) and the International Criminal Tribunal for Yugoslavia (United Nations).

⁴⁶ (United Nations, 1948)

Operational Considerations

Strategic

Any military operation must support the overall strategic vision. While this statement may seem banal in the context of modern hostilities, it assumes a different significance in the realm of cyber activity. Most of the external cyber activity occurring today that concerns the United States does not occur in conjunction with physical warfare. Rather it is between rival nations who enjoy normalized, relatively peaceful relations.⁴⁷ For this reason, there are two different strategic dimensions to external cyber activity.

First, consider national strategy. The Obama Administration's 2010 National Security Strategy emphasizes four "enduring national interests": security, prosperity, values and international order.⁴⁸ Policy for external cyber activity needs to support these principles without undermining any one of them. For instance, employing a cyber counterattack that seeks to promote our security and prosperity, but which destabilizes the international order, would be a strategic miscalculation. This is a significant consideration for U.S. cyber policy toward advanced persistent threats (APT). With regard to the Libyan example above, the *New York Times* reported that NATO's decision to refrain from using cyber weaponry was partially a function of the danger of setting a precedent. This decision demonstrates the importance of supporting national strategy in electing to use external cyber operations.⁴⁹

⁴⁷ For example, See (McConnell, Chertoff, & Lynn, China's Cyber Theivery is National Policy - And Must Be Challenged, 2012)

⁴⁸ (The White House, 2010)

⁴⁹ It is also a fitting example of the interaction between strategy and economics. Though economic considerations may end up justifying the acceptance of strategic risk, policy makers evidently decided to bias toward supporting strategic imperatives.

There is also an interaction between national strategy and theater strategy. DoD defines theater strategy is “an overarching construct outlining a combatant commander’s vision for integrating and synchronizing military activities and operations with the other instruments of national power in order to achieve national strategic objectives.”⁵⁰ Cyber operations conducted in support of a theater strategy have greater potential for impacts affecting U.S. national strategy and accordingly require additional national oversight.

Executional

Policy-makers must account for various operational considerations. First, in conventional warfare, the mere existence of a weapon, weapon system, unit, etc. is in itself the presence of a capability. While the U.S. may not acknowledge the existence of some weapons, the capability still exists and they are available to commanders or policy makers for promoting national security. And, use of a conventional weapon (classified or otherwise) generally does not limit potential future use.

Such is not the case for cyber capabilities. All external cyber operations are predicated on system vulnerabilities.⁵¹ To conduct a cyber operation an organization must first identify a vulnerability, and then develop and test an exploit to achieve the desired effects—creating a cyber capability. Use of a cyber capability inherently risks disclosing the existence of the exploited vulnerability, thereby allowing the adversary, and potential future adversaries, to correct the underlying vulnerability. Essentially, once a cyber capability is used, it is possible that the operational capability may quickly vanish as vulnerabilities are remediated.

⁵⁰ (U.S. Joint Chiefs of Staff, 2012)

⁵¹ (Lin, 2010)

For this reason, cyber action has special Executorial considerations that are highly context dependent. Also, here lies another example of the complex nature of cyber policy. If a commander is weighing options to use an available cyber weapon, he/she must also factor the national implications of possibly losing that operational capability in the future.

Additionally, operational options must be cost-effective. Though governments should always be responsible in the expenditure of public funds, the recent financial crisis has raised this imperative to a higher level in the collective consciousness. Austerity measures in many European countries⁵² have often resulted in major cuts in government spending in order to close budget deficits.

Spending on cybersecurity, however, has remained an exception, not only because of the perceived severity of the threat, but also because of the perceived possibility for cyber action as a *cost-effective alternative to conventional weaponry*.⁵³ After a decade of elevated defense spending, frugality is once again becoming a major Executorial consideration. For instance, when questioned about NATO's decision not to use cyber weapons in Libya⁵⁴, a senior strategist replied that the decision might be different in the future for economic reasons. According to the strategist, the high cost of a conventional attack (including the weapon system and rebuilding the target that was destroyed kinetically) now makes cyber options more attractive. Thus, the potential cost advantage of cyber action is a critical Operational consideration for cyber policy formation.⁵⁵

⁵² (BBC News, 2011)

⁵³ (BBC News, 2010)

⁵⁴ (Schmitt & Shanker, 2011)

⁵⁵ A salient example is Eisenhower's choice of nuclear deterrence as a means of ensuring global peace. Eisenhower believed that maintaining a numerically and technologically superior force to the Soviets' would not be feasible economically. The deterrence option, he believed, was more

Temporal

Commanders desire the ability to achieve instantaneous effects for greater operational flexibility. This seems particularly apropos in cyberspace where milliseconds is the standard unit of time. Code initiated on one part of the globe can reach the other side within seconds.

Unfortunately, the reality in cyberspace is more nuanced. Cyber operations have aspects that are both slow and fast. The execution of a particular cyber attack can produce effects milliseconds after the execution order. However, the operational planning, preparation, and conduct of a sustained cyber operation can be a much slower process.

For instance, evidence suggests the Stuxnet virus was first deployed in June 2009, but did not take effect until the following year.⁵⁶ In this instance, expediency was not a driving factor. The cyber attackers could afford a degree of patience. This may not always be the case. Thus, a major consideration for using external cyber operations is the desired timeframe of effects and insuring the policy, legal, and decision making process does not unnecessarily inhibit cyber action that needs to happen on the scale of milliseconds.

Consequential

Domestic

There are various domestic considerations for external cyber activity. First, as noted in the ethical considerations section, the American populace is

cost effective. See (Ambrose, 1984) Though we are not necessarily suggesting an era of cyber deterrence, this is also a particularly germane example in that the moral and strategic implications of Eisenhower's decision were exceptionally complicated.

⁵⁶ Additionally, further examination of the code revealed that it had been updated at least two more times before finally reaching its target. (See, Zetter, *supra* note 8)

notoriously wary of privacy infringement and distrustful of government monitoring. Despite the growing push by lawmakers for increased Internet monitoring by the Department of Homeland Security (DHS)⁵⁷, the need to respect individual privacy has remained of paramount concern. Defensive cyber operations, like the Department of Justice and FBI's takedown of the Coreflood botnet, which contained over 2 million infected systems, required extensive legal justification.⁵⁸ This reflects the domestic political sensitivity of government influence (or some may say intrusion) on private citizens' lives.

Additionally, there are interagency political issues that complicate uniform cyber policy. DHS has the responsibility to protect U.S. citizens within the borders, but the vast majority of cyber resources reside at NSA and DoD. A 2009 National Research Council (NRC) report suggests that military external cyber operations would have implications for other agencies' missions (including DoS and Treasury).⁵⁹ A consideration for policy makers, therefore, will be the facility in aligning these various interests.

Lastly, the authorization for the use of force constitutionally rests with Congress. Should an agency decide to engage in external cyber operations that could be considered a use of force, it may require Congressional approval. Achieving this politically (and expeditiously) may prove problematic. This suggests that the need exists for establishing pre-approved authority levels, and having a robust debate to establish norms for acceptable cyber action.

⁵⁷Though terrorist organizations have leveraged the power of social media, DHS has made it abundantly clear that they wish to protect individual privacy. They claim that current monitoring is in accordance with "defined parameters articulated in published department privacy guidelines." (Hosenball, 2012)

⁵⁸ (James, 2011)

⁵⁹ (National Research Council, 2009)

International

Multilateral action is often more effective in achieving U.S. national interests, making international politics a critical consideration. Currently, external cyber operations remain classified, but should such operations rise to the level of cyber attack, it would be critical for the U.S. to seek multilateralism. This act of legitimacy-seeking may require not only coordination with allies bilaterally, but also the United Nations and potentially NATO.

Assuming that there are diplomatic agreements, external cyber operations will require coordinating with allied forces. More than 30 nations have cyber units in their armed forces⁶⁰, many of which are our allies. These nations with capable units are inevitably conducting external cyber operations of their own. A U.S. decision to take significant action in cyberspace may interfere with our partner nations' efforts.⁶¹ To avoid potential conflict, the U.S. must consider the Operational coordination required to ensure proper deconfliction. Depending on Temporal considerations, this may adversely affect the decision to use cyber technology.

Finally, as an emerging domain, setting international norms for behavior and conduct in cyberspace is a key policy consideration. In making external cyber policy decisions the U.S. must consider the principle of reciprocity and see policies as an opportunity to establish norms and customary international law in cyberspace. The U.S. should prefer policies that are also acceptable to the U.S. as an international norm.

⁶⁰ (Wolf, 2011)

⁶¹ (See, National Research Council, *supra* note 20)

Soft Power

The U.S. must be able to project the second and third order effects of conducting external operations in cyberspace. One critical example would be the soft power implications for such operations. Specifically, most civilian global perceptions of the Internet (especially in light of the Arab Awakening) focus on peaceful uses. External cyber operations or other actions that may affect normal cyber activities, therefore, can adversely affect America's soft power.

A recent example of this is the Egyptian protesters' reaction to the Bay Area Transit Authority's (BART) shut down of cell service in one of their stations in August 2011. In anticipation of a protest at one of its stations, BART officials halted cell service in order to minimize the gathering. Many Bay Area citizens viewed this as a limit on their right to peaceful assembly. Egyptian activists from the Tahrir Square demonstrations seemed to agree. They began voicing their disapproval by referencing BART in tweets as "MuBARTak."⁶² Likening BART's actions to those of the deposed president reflects a certain loss of prestige abroad, signifying an erosion of soft power.

In that vein, the U.S. must consider the implications for external cyber operations in affecting perceptions of the U.S. abroad. A cyber action that is Executionally or Strategically expedient may have second or third order effects that diminish American soft power.

Systemic

Cyberspace is a unique domain where, unlike the domains of land, sea, air, and space, the very geography and "laws of physics" can change by disconnecting systems or changing the protocol or code that operates cyberspace.

⁶² (Hersh, 2011)

Potential changes to the “laws of code” in response to external cyber action may fundamentally alter the nature of cyberspace and render a large set of existing cyber capabilities obsolete.

Cyber policy makers must carefully consider the systemic effects of their policies. How will civil society organizations, such as the Internet Engineering Task Force (IETF), react to a cyber action? How will the political economy of cybersecurity change if organizations are free to conduct cyber attacks? Can the Internet survive as an interconnected and global commons if it becomes a domain used to conduct frequent military strikes?

Currently the incentive structure in cyberspace systematically favors attackers over defenders. Correcting this misaligned incentive should be a key consideration of cyber policy makers in order to mitigate the risks of external cyber actions’ producing undesirable systemic effects. We believe it could be accomplished through the application of deterrence and mitigative counter-attacks to stop cyber attackers. Improving security in a manner that does not diminish the tremendous openness and generativity of the Internet, but instead increases it, is the essential goal of cybersecurity policy.⁶³

Use of the Framework

Many of the ten considerations overlap and affect each other. We have suggested some examples of overlap in the descriptions above, but it should be obvious that acting without due regard for all the considerations could result in unintended consequences. An operationally sound and legal external cyber operation that is not coordinated politically internationally may strain relations abroad and undermine core principles of the national security strategy.

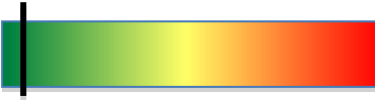
⁶³ (Zittrain, 2009)

Conversely, a cost-effective external cyber operation that has been coordinated with allies abroad but which is arguably unethical could erode the nation's soft power.

From this vantage point, it is evident that sound policy will balance these considerations and account for all of them. Though this may be true for any DoD policy, it is especially true in cyberspace due to its relative infancy and its complex nature. Our recommendations that follow flow from these considerations and reflect our viewpoints of each external cyber activity.

IV. Cyber Actions with Minimal Effect

Scanning:

Cyber Action	Overall Severity of Implication	Recommendations
Scanning		<ul style="list-style-type: none">• Establish interagency understanding that scanning is good intelligence practice.• Do not describe scanning as “attacks.”• Conduct with good operational security.• Establish process to share identified vulnerabilities when appropriate.

Description

Scanning is the act of checking or scanning for security vulnerabilities. This category explicitly excludes any conduct that involves actually gaining access to the computer system, which we categorize as an intrusion. Instead this category is best exemplified by actions such as port scans and route tracing.

In many policy discussions, scanning is often reported as a “cyber attack”,⁶⁴ when in reality it is much more akin to observed suspicious activity. This imprecise description is resulting in substantial exaggeration of the present cyber threat. Scanning is often conducted by security researchers in an automated fashion to test for how widespread known security vulnerabilities are, but also by malicious users who are seeking to gain access to systems. Simple scanning and determined attempts at accessing a computer system may be indistinguishable. This category is the most benign form of external cyber action which we analyze.

⁶⁴ (See, Collins, *supra* note 26)

Policy Analysis

Normative Considerations

Ethical

Scanning poses few significant ethical concerns. It causes no harm to the “victim,” and scanning can be conducted for very benevolent purposes (e.g. to inform a victim that he/she is vulnerable to cyber attacks). Only under the broadest notions of privacy could one view scanning as offensive, because the act of connecting a computer system to a publically accessible network certainly suggests an acceptance for communication based upon basic protocols.

Individuals acts of scanning conducted as part of an operation can result in a denial of service type attack. However, such an action would be amount to a cyber attack in that it causes disruption.

Domestic Law

On initial analysis, scanning may present legal issues in three areas: 18 U.S.C. § 1030 – the Computer Fraud and Abuse Act (CFAA), authorities for military and intelligence actions domestically, and the 4th Amendment. There may be other areas of law worth considering that are beyond the scope of this project.

While the military and intelligence agencies are limited in their domestic actions, they are not absolute prohibitions. FISA, 50 U.S.C. § 1801, is defined only to protect U.S. persons when there is a reasonable expectation of privacy and a warrant would apply for law enforcement. This would not be the case for scanning computers on a publicly accessible network. While the military is prohibited from domestic law enforcement, it is permitted to support civil authorities. Regardless, scanning is not an act of law enforcement.

The 4th Amendment protects against unreasonable searches and seizures. For a computer connected to a public network, it is difficult to see how scanning could be considered an unreasonable search. As such the 4th Amendment poses no substantial concerns.

Scanning poses few significant ethical concerns. It causes no harm to the "victim", and scanning can be conducted for very benevolent purposes.

Scanning could be found to be illegal under the CFAA only with particularly broad interpretation of the phrase "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains...information from any protected computer."⁶⁵ Suggesting that requesting and receiving readily available information from a computer system connected to a publically accessible network is to "accesses a computer without authorization or exceeds authorized access" is a very expansive interpretation that strains principles of statutory interpretation.⁶⁶ The most restrictive standard that courts are applying for what conduct is considered "without authorization" is that which is not "in line with the reasonable expectations" of the website owner and its users.⁶⁷ Under such interpretations scanning certainly seems permissible.

Perhaps the strongest indication that scanning is permissible under domestic law is the United States Federal District Court in Georgia ruling in *Moulton v. VC3* where the judge declared a port scan legal because it did not

⁶⁵ See 18 USC. § 1030(a)(2) accessed here (http://www.law.cornell.edu/uscode/pdf/uscode18/lii_usc_TI_18_PA_I_CH_47_SE_1030.pdf)

⁶⁶ (See, National Research Council, *supra* note 20)

⁶⁷ For an analysis of the CFAA see (Electronic Frontier Foundation, 2010)

“impair the integrity nor availability of the network.”⁶⁸ It is indeed challenging to see any substantial concerns regarding scanning under domestic law.

International Law

We find nothing under international law that would limit cyber scanning.

Operational Considerations

Strategic

The minimal effects of scanning suggest it poses few strategic implications. Scanning, at worst, is an extremely innocuous form of intelligence collection. It is difficult to imagine any substantial strategic considerations beyond the executional considerations.

Executional

Scanning can provide information to the target and as such poses some executional considerations. Scanning can indicate the systems of interest, the vulnerabilities of interest, and (if poorly executed) the origin of the scan (both the computer system and the actor). Due to the high number of automated systems currently conducting scanning and attacks,⁶⁹ there is a high amount of background noise to mask any scanning activities. While this poses a severe challenge to defensive action, it does allow for the masking of external actions.

These executional considerations are best approached through a standard “intel gain/loss” framework. While there may be potentially strategic implications, this is certainly no argument for any policy prohibition on scanning. Intelligence agencies have established practices for managing

⁶⁸ (Moulton v. VC3, 2000)

⁶⁹ (Bloomfield, Gashi, Povyakalo, & Stankovic, 2008)

operational intelligence collections considerations that should make a straight forward translation to cyber scanning. Good tradecraft can mitigate all the executional concerns we have identified.

Temporal

Scanning a computer system to detect its potential vulnerabilities is conducted on the scale of seconds. However, identifying computer systems and targets of interest requires a lengthy period of intelligence collection. Moreover, capability to conduct detailed scanning with good tradecraft takes potentially years to develop. These time constraints suggest that to ensure freedom of operation in cyberspace and the ability to conduct strikes at a time and place of choosing, then scanning should not be restricted by policy and decision making time cycles, and should be seen as a routine and ongoing intelligence collection activity.

Consequential Considerations

Domestic

Scanning, particularly if it affects U.S. persons, certainly has the potential for raising domestic political concerns. Being the first step to information collection or more sophisticated cyber attacks, scanning may raise concerns of government spying and privacy infringement on the U.S. population.

These concerns may be greatly mitigated if scanning is conducted within a framework of security information sharing. Certainly the focus of any scanning by DoD would be on foreign agents, but should U.S. government agencies identify computer vulnerabilities on citizens' networks, the U.S. government can choose to inform the operator, perhaps through DHS or law enforcement authorities that have a tradition of working with the private sector to correct security vulnerabilities. Clearly any such effort would have to correspond with

careful decisions regarding: declassification, operational impacts of information sharing, the avoidance of any sort of market distorting impact (such as establishing favored organizations), and the adverse potential for forming a dependency in U.S. network operators who may perceive a government certification as a guarantee of security.

Beyond the potential privacy concerns there are few domestic political or public concerns that seem likely to be raised by scanning.

International

Given the high level of scanning going on by criminal and other actors it seems unlikely that foreign governments would raise concern regarding scanning. It seems likely that such activity is already being conducted at a high volume by state intelligence services, so it is hard to imagine substantial international consequences to scanning.

Soft Power

The principle soft power consideration is similar to the domestic considerations concerning a perceived infringement on privacy, and a resulting loss of esteem for the United States. But again, the high amount of scanning activity already being conducted, and without much notice, suggests that it would both be easy to mask any government scanning and there would not be severe concern if it became known. Indeed there is already such a perception of powerful U.S. surveillance capabilities in much of the world; it is hard to see a substantial shift caused by external scanning efforts.

Systemic

More scanning for security vulnerabilities is likely to have a positive systemic effect on the internet, making it more secure in general. As more

security vulnerabilities are identified and recognized, organizations will seek to identify and correct these vulnerabilities contributing toward the U.S. objective of a more “trusted and resilient” net.⁷⁰

Example Scenario

To synthesize the above considerations, consider this scenario which includes both reacting to and conducting scanning:

Network administrators at DoD observe an unusual pattern of network activity with computers external to the DoD network frequently attempting to establish connections to a specific set of ports on DoD’s Internet-facing systems. The administrators concerned that these attempted connections may be an effort to exfiltrate data from the DoD network take defensive measures to ensure no DoD computer is communicating to the Internet on these ports. Seeking to better understand the threat they request⁷¹ to conduct scans of the machines attempting to connect to the DoD network to ascertain basic information like they’re location on the Internet, and the operating systems they are running.

Normatively, there are little significant concerns with conducting these scans. The one area that may give some pause is domestic legal constraints. If the external computer’s conducting the scans have 4th Amendment protections, then there might be reasons to constrain the action. However, without conducting a scan DoD is unlikely to have any information that indicates the location of the machines. Moreover, as long as the information being obtained isn’t private information, and the methods don’t constitute an unreasonable search, there is

⁷⁰ (The White House, 2009)

⁷¹ Most network administrators are likely to conduct these scans without requesting authorization, unless otherwise restrained, because they are of such a basic and routine nature.

no reason for concern. It certainly seems the case that conducting a scan meets these criteria.

Operationally, care is needed, in responding to the scanning activity and DoD conducting their own scans provides information to a potential adversary. First, it indicates DoD detected the scans. It may be better to ignore them and lull the potential adversary into a false sense of capability. Second, DoD may wish to conduct its scans using deniable computers to avoid revealing its action or indicating additional systems used by DoD (which could then be the target of cyber action). Such operational concerns are best managed by intelligence professionals who can balance the intelligence gain/loss of active or passive counter-intelligence collection, and is not a concern for policy makers.


The consequences would be the least desirable in the case where the external computers scanning the DoD network are not owned by the perpetrators, but have been infected with a computer virus. In such a case it is possible that the organization that owns the computers may notice their computers *being* scanned but be unaware that their computers are *conducting* scans of the DoD network. This could be harmful to the U.S. in international relations if this “middle man” is in fact a foreign government. This risk is partially mitigated by using deniable computers to conduct external action, but can be better handled if the U.S. has a mechanism for cyber-insecurity information sharing and can communicate to the affected organization that they may be infected with a computer virus, and work with them to correct the issue.

Policy Recommendations

Scanning presents no ethical or substantial legal concerns; however, it does pose some political and operational issues. As such, it should be conducted within some policy oversight to:

- 1) Establish an interagency understanding that scanning is a part of good, modern cyber intelligence practice and due to its benign nature should be minimally constrained.
- 2) Avoid exaggerated policy rhetoric that describes scanning as attacks. While this is accurate in computer security parlance, it is highly confusing in the policy debate and greatly exaggerates the threat faced.
- 3) Encourage good trade practice in conducting external scanning activities. Operationally try to avoid scanning of systems owned by U.S. persons, but recognize that such collection is permissible.
- 4) Have a process to share identified vulnerabilities with the owner of the vulnerable system when appropriate. This will require some declassification and consideration of operational impacts, but also setting up a politically acceptable information sharing process. Recommend conducting any information sharing through DHS law enforcement agencies.
- 5) Responding to cyber scanning is principally an operational intel gain/lose consideration, it is not a policy concern. Taking external action beyond scanning or efforts to determine the origin in response to scanning is ill-advised. Better to analysis the information provided by being scanned to prepare defensively.

Intrusion:

Cyber Action	Overall Severity of Implication	Recommendations
Intrusion		<ul style="list-style-type: none">• Conduct only to improve cyberspace security or support higher U.S. strategic objectives.• Establish disclosure procedures for sharing identified vulnerabilities, when appropriate.• Amend the CFAA.• Employ signaling in intrusions when able.

Description

A cyber intrusion is the unauthorized access of a computer system. Many computer systems are ineffectively protected. Gaining unauthorized access may be a trivial task that does not require any sophisticated capabilities, but yet may have potentially severe implications. We have isolated this category of external actions from attacks or those with information effects (such as information collection), because, even without any exploitation or harm being caused, the intrusion in of itself poses ethical and legal complications. It is important to recognize that while many external cyber actions require an intrusion (particularly cyber attacks and cyber force), not all do. For example DDoS does not require an intrusion.

Policy Analysis

Normative Considerations

Ethical

The unauthorized access of a computer system violates principles of agency. Despite no measurable harm being caused, this violation of another

individual's agency must be justified by some more substantial moral concern. Under a strict consequentialist frame of reasoning one concludes that even a small expected net benefit would be enough to offset the harmless violation of another's agency. While we do not advocate such a severe perspective, the basic calculus remains the same: there is a trade-off between the expected benefits from violating another person's agency and the value of respecting it.

There is a further ethical concern in that a prerequisite to conducting any intrusion is knowledge of a vulnerability. Given the commonality of information technology, if you know a vulnerability exists it is likely that the U.S. government and citizens, those the U.S. has a duty protect, also share this vulnerability. Intentionally allowing a vulnerability to persist and not informing the vulnerable party or the software creator is a morally tenuous position. This position can only be ethically justified by a clear higher moral purpose being served in maintaining the secrecy of the vulnerability.

Domestic Law

Intrusions pose substantial legal issues under 18 U.S.C. § 1030, the CFAA. These issues extend to all of the more severe categories of external cyber, and so are worthy of substantial analysis here. According to 18 U.S.C. § 1030 (a)(2), it is illegal for anyone to:

(2) Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section [1602 \(n\)](#) of title [15](#), or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act ([15 U.S.C. 1681 et seq.](#));

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

The term “protected computer” is defined in (e)(2) as a computer:

- (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or*
- (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.*

The application of § 1030 is only limited by (f):

- (f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.*

Applying a plain meaning interpretation of the statute, (a)(2)(C) amounts to making all acts of intentionally accessing a protected computer without authorization or exceeding authorized access illegal. This is because the act of accessing inherently entails the receiving of information, the computer “handshake,” in establishing access. The statute is not limited to obtaining “protected information,” so even obtaining routine accessing information is illegal.

As amended by the National Information Infrastructure Protection Act of 1996 “protected computer” takes an extraordinarily broad definition. All computers used for foreign communication are “protected”. This suggests that any computer in use outside of the U.S. is inherently protected, and any computer within the U.S. is protected if it is used in interstate or foreign communication. Simply put any computer on the Internet and any computer located in a foreign country is protected.

Finally section (f) exempts only law enforcement and intelligence agencies from the limitations imposed by the statute. There are two ways of interpreting this: *Ejusdem generis* (of the same kind) or *Expressio unius est exclusion alterius* (the mention of one thing excludes all others). That is, is the mentioning of law enforcement and intelligence agencies trying to illustrate a class of actors (including the military) that are exempt from the statute? Or is it specifically limiting the exemption to those two kinds of actors? The language of (f) suggests it is limiting the exemption just to law enforcement and intelligence agencies. **This means that any unauthorized access of foreign computers by the military illegal.**

This restriction is likely an unconstitutional violation of the Presidential powers granted by section 2 of the U.S. Constitution. But, in the absence of a clarifying decision, the CFAA limits what the military may engage in and what sorts of policies can be established in the conduct of cyber operations.

Further domestic legal restrictions are similar to those mentioned in the discussion of scanning. In particular, there is a clear expectation of privacy in at least the case of circumventing a protection measure to access a computer. Thus 4th Amendment protections do apply in cases involving U.S. people. Cases where the access to the computer is unauthorized, but no protection measure is circumvented, is not as clear a violation of the 4th Amendment because there may be no reasonable expectation of privacy for a computer system without any protection measures.

International Law

Many states have laws that prohibit the unauthorized access of computer systems. Article 2 of the Council of Europe Convention on Cybercrime,⁷² which the U.S. has signed and ratified, reads:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

How Article 2 is implemented in the laws of the 46 signatories to the convention and to the extent it applies to national government actors, is an interesting subject for further inquiry beyond the scope of this project.

The various domestic implementations of the Budapest Convention on Cybercrime are a foundation for inferring an emergent customary international law. Moreover, the U.S, as a signatory, has a clear obligation to see the tenants of the Convention as customary international law and respect it as such.

Fortunately, the convention is much more limited in scope than the CFAA, criminalizing an intrusion only if it is “committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.”⁷³ However, even this may place unacceptable restrictions on U.S. intelligence or defense action, and the U.S. may need to look to legally justify external cyber actions based on the convention’s focus on criminal activity and

⁷² (See, Council of Europe, *supra* note 40)

⁷³ (See, Council of Europe, *supra* note 40)

argue it is not intended to limits on the actions of the state. There is merit to this argument, especially if the U.S. can demonstrate that states, especially signatories to the convention, are engaged in international cyber action that violates the convention.

Operational Considerations

Strategic

The U.S.'s International Strategy for Cyberspace establishes as a strategic goal a secure cyberspace.⁷⁴ Conducting intrusions is a first order operation that undermines this strategic objective. Further to the extent that there is a customary international law against cyber intrusions, conducting cyber intrusions undermines the international rule of law; this violates one of the national interests of the United States: to promote an international system that respects the rule of law.

This is not to say intrusions are strategically inadvisable. Conducting a cyber intrusion would be strategically acceptable if conducted to achieve some higher strategic purpose or secure more important national interests. Furthermore, a cyber intrusion could be conducted in order to promote a more secure Internet, for example in stopping an ongoing cyber attack or a pending attack through the involuntary removal of malware or through a botnet takedown. Cyber intrusions conducted for the purpose of creating a more secure Internet pose no contradiction with the U.S. International Strategy for Cyberspace.

Intrusions should only be conducted when they can be expected to improve the security of cyberspace or be in support of a higher-order U.S. Strategic objective.

⁷⁴ (The White House, 2011)

Executional

Intrusions share all the Intel Gain/Loss sort of considerations as probing. Additionally, intrusions raise an issue in signaling and uncertainty regarding intent and effects of the intrusion. The victim that identifies he has experienced an intrusion is likely unable to determine what the intent of that intrusion is or what was affected. The victim is likely to exhibit a worst-case bias and assume the worst: Intrusions are treated like attacks. This results in a potentially escalatory cycle. To avoid this, attackers should seek, when possible and appropriate, to signal the intent of an intrusion—for example, by gaining/using read access instead of root access on the compromised system. Alternately, intrusions on critical systems that control physical systems and could result in physical effects that amount to a cyber use of force should be avoided.

To conduct a cyber intrusion also requires knowledge of some vulnerability. Given the commonality of information technology, it is likely that critical systems in the U.S. share this vulnerability. Identifying but not correcting vulnerabilities places the U.S. in a precarious position; instead of exploiting vulnerabilities, it may be operationally wiser to work with software vendors to correct them.

Temporal

To conduct collection or an attack, access to the computer system must first be achieved. This means there is an operational synchronizing aspect, whereby to have the capability to conduct an attack at a time of choosing one must have conducted an intrusion on the targeted system. This is an important operational constraint. Conducting the intrusion to ensure you have the capacity to conduct an attack risks informing the adversary of his/her vulnerability and the vulnerability you plan to exploit. The implication of this is that multiple

intrusion methods are required to ensure the success of an attack: exploit one vulnerability to ensure you have access and know the system's vulnerabilities, and then use a separate vulnerability to conduct the actual attack in case the vulnerability used in the initial intrusion is repaired.

This temporal constraint suggests a continual state of cyber intelligence collection where new methods of conducting intrusions on potential targets are tested to ensure an operational capability. This is a challenging situation considering the ethical, legal, and strategic concerns identified above, where intrusions are being conducted just to ensure an operational capability and not for a more substantial ethical or strategic purpose. Is continually conducting intrusions acceptable conduct for the U.S? The U.S. likely needs to restrain the conducting of intrusions and accept a degraded and less assured operational capability, to properly balance these competing interests.

Consequential Considerations

Domestic

The domestic audience is certain to perceive the conduct of intrusions as aggressive action that impinges on privacy. As such it is vital that intrusions are conducted under political oversight that ensures the conduct is justifiable for strategic ends and in a manner that minimizes the impact on the U.S. population and civil liberties. The U.S. population is likely to find most acceptable the conduct of cyber intrusions against threatening nations and groups. The least tolerable of intrusions are those against U.S. citizens, civil actors, and allied countries.

International

Nation states are certain to react unfavorably to any known intrusion. It is tempting to compare intrusions to other forms of espionage; however, the

potential for an intrusion in critical systems to result in widespread systemic damages makes it qualitatively different. To avoid this complication, it is important that intrusions are discriminate. An intrusion on a purely information system is qualitatively different from one on an industrial control system. Achieving this level of discrimination poses an added cost on cyber action.

There is also an issue of international norms and customary law. Right now there is an emerging customary law that condemns all intrusions. However, there are good and benevolent reasons to conduct an intrusion, such as automated removal of a botnet. The U.S. may wish to move the international norm towards a more narrow prohibition, perhaps against intrusions that cause harm or intrusions that circumvent a protection measure in order to cause harm. There is some foundation for this more proscribed formulation in the Budapest Convention on Cyber Crime, but this is not reflected in U.S. law and the law of some other countries.

Soft Power

The public has an expectation of privacy on its computer systems. This is perhaps unreasonable given the insecure nature of present day information systems. However, this expectation exists and any intrusion will be seen as a violation of the user's privacy, will undermine U.S. legitimacy abroad, and will contribute to a distrust of the Internet. The Internet, and other interconnected information sharing platforms are a powerful vehicle for the delivery of soft power influence. Any distrust in these systems, or a movement towards balkanization is damaging to U.S. soft power and influence abroad. The U.S. International Strategy for Cyberspace correctly recognizes this dynamic and wisely includes as a strategic objective maintaining a trusted and secure cyberspace.

Systemic

Despite the first order effect of conducting an intrusion undermining the security of the cyberspace, the second order effect is likely to improve the security of cyberspace. One of the fundamental problems in cybersecurity is that most don't recognize their vulnerability.⁷⁵ Conducting intrusions actually raises the awareness of the underlying vulnerabilities and incentivizes reducing both the vulnerabilities and the potential impact of intrusions. It is hard to imagine a stronger incentive for the IT industry to improve cybersecurity than the exploitation of vulnerabilities (even for beneficial purposes).

Example Scenario

To synthesize the above considerations, consider this scenario of deciding to conduct a cyber intrusion on a foreign computer system:

DIA receives information from a human source in a foreign navy that they have recently transitioned to a computer inventory system for their ordnance at a strategic port on a key international shipping lane. The U.S. has long been concerned that this nation may mine the shipping lane, which would severely disrupt global trade; therefore, the U.S. is very interested in learning what types and quantities of mines are being stored at this naval port. DIA's source has no information on the mines at the port, but knows mines and all other ordnance are tracked on this new computer inventory system, that this computer system is connected to the Internet, and he provides the IP address of the computer. Eager to confirm this information and learn more about the ordnance at this naval facility DoD considers accessing the computer system.

Inherent in this scenario is a degree of uncertainty: without actually accessing the indicated computer system DoD cannot be sure of who owns the

⁷⁵ (Moore, 2010)

computer at the provided IP address and what the computer system is used for. Conducting a Cyber Intrusion on the provided IP address is the first step for any additional intelligence collection, or even operations to disrupt their capability.

Ethically, the purpose of the operation is to prevent the mining of an important shipping lane. This constitutes a higher moral purpose that overrides the potential for privacy infringement should the IP address actually belong to a private individual.

Under domestic law, this activity is authorized if conducted under intelligence authorities, and not military authorities, as this intrusion clearly constitutes an unauthorized access of a computer involved in foreign communication, which is prohibited under the CFAA. To further protect U.S. persons, there should be a policy to discard all information achieved if it is discovered to be a computer of a U.S. citizen. Even if following the language of the Budapest convention as international customary law, this intrusion is legitimate under international law.

Next examine the Operational considerations. Strategically, this intrusion supports a national interest in protecting international trade, which is likely a higher order interest than promoting a secure and trusted cyberspace. Operationally, there is the risk in conducting the intrusion of the intrusion being detected (perhaps in the future) and the inventory system being taken down. Additionally, the method and vulnerability exploited to conduct the intrusion may be discovered and corrected in this system and others. However, these risks are likely worth assuming in order to confirm the intelligence and potentially acquire information on the ordnance inventory. Temporally, so that any action or additional collection can take place as needed in the future, it is essential to immediately confirm the nature of the computer system and that gaining access

is possible. The capabilities used to gain access in a clandestine manner must have already been developed.

While there are a number of potential consequences of this action as others react, they all tend to be minor. Perhaps most severe, however, is that if this intrusion were publically discovered as conducted by the U.S. government, it could possibly lead to national militaries' reducing their presence in cyberspace. This in turn might reduce the U.S.'s ability to conduct cyber operations internationally in the future. If the IP address turns out to be a private individual, and again the intrusion is attributed to the U.S., there is the risk that the U.S.'s image abroad could suffer. If just the intrusion is discovered, but not that it was a U.S. action, then the principle consequential impact is the systemic effect of actors looking to better secure their information systems, which, while impacting U.S. cyber capabilities, also reduces all other's capacity for external cyber action and contributes to the U.S. strategic objective of a more secure cyberspace.

Conducting this intrusion seems certainly permissible. The Operational and Consequential considerations are similar to other intelligence activities (also suggesting that this operation have similar oversight). This action also comes close to the legal limits of CFAA domestically. The operation also demonstrates the need to constrain emerging international customary law on unauthorized access to computers to ensure legitimate activity does not become legally prohibited.

Policy Recommendations

- 1) Intrusions should only be conducted when they can be expected to improve the security of cyberspace or in support of a higher order U.S. Strategic objective. Policy makers should develop a framework to guide this assessment.

- 2) Policy oversight is required to determine when the U.S. is best served in disclosing an identified computer vulnerability to try and correct it, and when it is best to keep the vulnerability secret for future exploitation.
- 3) The CFAA needs to be amended, while remaining consistent with the Budapest Convention on Cybercrime, to clarify the statute's applicability and to distinguish between what is outlawed from what is objectionable.

Specifically we recommend the following amendments:


- a. Protection for foreign computers needs to be weakened. The definition of protected computer, (e)(2)(b), should be changed to "which affects the operation of critical infrastructure important to the United States, including public utilities, communication systems, financial institutions, and public safety systems, even if that computer is located outside the United States.
- b. Criminalizing computer access "without authorization"⁷⁶ cedes too much authority to private actors, allowing them to criminalize action through Terms of Service (TOS). Statute should instead criminalize only the circumvention of a security measure; amend (a)(2) to "Intentionally circumvents a security measure to accesses a computer, without authorization or exceeds authorized access, and thereby obtains —"
- c. Amended (a)(2) (a), (b), and (c) by replacing "information" with "protected private information." Where private means that information which is not publically available and protected meaning the holder of the information has made positive steps to prevent the information from being publically known.

⁷⁶ (See, 18 U.S.C. § 1030 (a)(2), *supra* note 63)

- d. Section (f) should be expanded to exempt the lawfully authorized activities of the U.S. Military and Department of Homeland Security from prohibition.
- 4) Customary international law on cyber-intrusions is emerging. U.S. should work to set a norm that is not overly restrictive. An overly restrictive international legal standard would bind the legitimate actions of law-abiding nations and increase the vulnerability to rogue actors.
- 5) Consider signaling dynamics in intrusions; when possible signal the limited scope of an intrusion to avoid the risk of escalatory cycles.
 - a. Similarly, be careful in responding to detected intrusions to avoid over-reaction.

V. Non-Disruptive Cyber Actions

Data Collection:

Cyber Action	Overall Severity of Implication	Recommendations
Data Collection		<ul style="list-style-type: none">• Ensure protection of privacy.• Promote reasonable norms for privacy protection standards.• Continually fund research of new TTPs.

Description

Cyber Data Collection (DC) is the deliberate collection of protected private data. “Protected” means it is information that is subjected to a deliberate effort to keep it out of the public domain; and “private” means it is information that is in fact not in the public domain. DC doesn’t require an intrusion. For example, monitoring of communications or other SIGINT collection activities may be sufficient. In addition, it may be possible to deduce what is considered protected private information through large-scale collection and analytics, for example with big data analytics tools like Palantir.

Policy Analysis

Normative Considerations

Ethical

DC is inherently a violation of privacy and of agency. DC violates agency in that the information is under deliberate protection. DC violates privacy in that the information is clearly considered private. The protection of the information

indicates a will to keep the information secret. Violating this desire and another's agency requires a moral justification.

Beyond issues of agency, there is the concern of respecting privacy. Defining precisely the normative right to privacy is a complex and multifaceted debate, which is the subject of substantial ethical reasoning and debate.⁷⁷ However, it is generally agreed that there exists some moral obligation to respect the privacy of other's information. As such this violation of privacy needs to be justified above and beyond the justification provided for violating another's agency, suggesting the need for a higher moral purpose and a more substantial ethical justification for the conduct of DC.

Privacy is a growing and complex concern in cyberspace; minimizing and mitigating privacy concerns is a primary challenge for any cyber intelligence collection.

Domestic Law

Regarding Data Collection of any form, the initial domestic legal concern is privacy and 4th Amendment protections. Cyber DC poses special and ambiguous challenges in this regard, due to a number of unanswered questions on what sorts of technical collection constitutes an unreasonable search. The 2012 Supreme Court Case of *United States v. Jones* regarding GPS tracking⁷⁸ avoided resolving some of the most challenging questions on this topic, and instead centered on the physical attachment of the device as the offensive act.

However, the domestic legal definition of unreasonable search is only of minor importance, as presumably the focus of DoD Cyber DC would be targeted at non-U.S. persons, and there are few limitations on such conduct. However, given that US intelligence authorities limits collection against US individuals, these questions still have some import in cases of incidental collection. If in a U.S.

⁷⁷ (Tavani & Moor, 2001)

⁷⁸ (*United States v. Jones*, 2012)

intelligence DC program a U.S. person's private information is collected incidentally and unintentionally as part of the collection process (a likely situation in cyber DC), but the collection method does not constitute an "unreasonable search," then there may be legal room to justify the program.

The scope of FISA and similar limitations are complex and politically charged legal considerations. These questions require detailed analyses by legal professionals. For this discussion we simply recognize that there are little domestic legal restraints on cyber DC on non-U.S. persons, and that there exists some ambiguous, but not absolute, limitations on cyber DC that collects data on U.S. persons.

International Law

The Universal Declaration of Human Rights (UDHR) Article 19 provides strong protections to the collection of information, stating: *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."* This right is only limited to the extent it conflicts with other human rights in accordance with Article 29 (2): *"In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society."*

Cyber Data Collection is simply a new form of espionage and faces few limitations, and enjoys some protection, under international law.⁷⁹ The only significant limitation under the UDHR on mere collection is Article 12's

⁷⁹ (Kish, 1995)

protections for privacy. However, the actual use of information collected, including sharing and dissemination, faces additional limitations under the UDHR and under international law regarding protection of property, copyright, security, and maintaining public order.

Operational Considerations

Strategic

The United States has two principle strategic objectives at odds with Cyber Data Collection: privacy protections and promoting a secure and trusted cyberspace. DC efforts must be targeted and conducted in a manner that minimizes the harm to these two strategic objectives, and ensures the strategic benefits are worth the negative consequences of the action.

The U.S. has repeatedly established protection of privacy as an important objective. The recent framework for Consumer Data Privacy in a Networked World⁸⁰ published by the White House is one recent example of the U.S.'s setting privacy protection as an objective in cyberspace. The U.S. should seek to avoid wholesale DC against individuals. Instead, DC should be targeted against only clear national security threats.

Even with the most stringent privacy protections, DC is a first order undermining of the perception of a secure and trustworthy cyberspace. However, the vulnerabilities and insecurity are already present and being exploited by criminal, malicious, and hostile actors. So, to the extent DC efforts are collecting useful information to combat malicious actors, those DC efforts are not undermining the security and trustworthiness of cyberspace for non-malicious users.

⁸⁰ (The White House, 2012)

Executional

Effective DC requires consideration of standard intelligence gain-loss concerns. Specifically, any collection effort has the potential to signal what data is of interest and methods used in U.S. DC. This results in the risk of becoming vulnerable to the target of the DC manipulating their data to create inaccurate results. Additionally, the information collected is valuable, and other actors may look to access the collected data to gain any of the insights the U.S. acquired through their data collection efforts. Finally sources of information may become closed as actors learn how valuable and exposed their data are and/or respond with other methods to the collection.

Temporal

Any information collection process must be an ongoing and enduring effort to ensure information is on hand when it is required. Cyber DC has additional constraints in that techniques to identify, access, and compile useful information must be continually researched, developed, and tested. Cyberspace is an evolving and changing domain. In all other domains the laws of physics control what is possible; however, in cyberspace the laws of code can continually be adapted and changed by engineers. Moreover, how users interact with and store data in cyberspace continually evolves.

Consequential Considerations

Domestic

The U.S. public has long been weary of the U.S. Government collecting intelligence on them. This is a particular challenge for cyber DC, because it is difficult to focus collection efforts solely on non-U.S. persons. To be politically acceptable, any DC program must avoid targeting U.S. persons, make proactive efforts to avoid incidental collection on U.S. persons, and limit the use of any

information on U.S. persons collected. This domestic political consideration leads to a challenging operational aspect, where adversaries will attempt to appear as U.S. citizens to avoid cyber DC. Balancing between this domestic and operational concern will require learning about the best practices of counter-intelligence organizations (who have direct experience dealing with this challenge) and applying these lessons to cyber data collection efforts.

International

The conduct of espionage and foreign intelligence collection is an accepted international norm, with most major states having multiple publically recognized agencies responsible for foreign intelligence collection.⁸¹ However, data collection in cyberspace raises special concerns, in that networks are voluntary in nature and can be altered. Data collection is likely to lead many states to balkanize portions of cyberspace to reduce vulnerability; the degree of this balkanization depends on the perceived evasiveness of data collection.

Concerns over possible vulnerabilities purposefully being inserted by state intelligence agencies in Huawei and Cisco routers are already leading France, in cooperation with other EU members, to seek the development of their own router manufactures. Fears of states conducting “supply-chain-poisoning” espionage activities may lead every state to develop its own IT infrastructure industry, turning IT into the new steel of international security affairs – where states see their own security dependent on maintaining an independent domestic industrial base. Such developments undermine global economic efficiency, the progress of globalization, and U.S. business interests.

⁸¹ (See, Kish, *supra* note 77)

Soft Power

Privacy is a growing and complex concern in cyberspace; minimizing and mitigating privacy concerns is a primary challenge for any cyber DC. Variable standards and norms for privacy make this an especially complex concern. European conceptions of privacy are particularly strong, with control of one's personal information being a strongly protected right. 74% of Europeans desire stronger controls of their data online and distrust corporate handling and use of their information.⁸² This intense level of concern over corporate use of online data would be minor compared to any sort of U.S. run cyber data collection program that was seen as infringing on privacy. Any such appearance would greatly harm U.S. image and soft power abroad, and may lead to individuals' reducing their use of the Internet, further reducing the U.S.'s cultural reach.

Systemic

Similar to intrusions, the second order effect of DC is likely to be a strengthening of cyberspace data protections. Such a consequence has a dual effect: further reducing DC capabilities, but also generating a more secure cyberspace. The U.S. as a technology leader should welcome such a development. As cybersecurity improves smaller actors, such as criminal organizations, terrorists, rogue states, and states with less technical capability than the U.S., are relatively diminished. The U.S. is asymmetrically both more vulnerable and capable in cyberspace; as such improving the security of cyberspace is strongly in the U.S.'s strategic interest.

⁸² (European Commission, 2011)

Example Scenario

The following scenario has been constructed to synthesize and illustrate the critical considerations of Cyber Data Collection:

As part of counter-terrorism efforts the U.S. government monitors a number of extreme Islamic jihadist forums that are publically accessible. On these forums individuals post technical information on bomb building, recruit members, upload pictures and videos of proposed targets and attacks, and claim responsibility for attacks. Some of these forums use publically available software that automatically logs IP addresses and other basic information of contributors, storing this for only the website administrator to view. An intelligence officer proposes conducting unauthorized access of the websites to collect the IP addresses of contributors, then investigating each IP address to link it with other behavior on the Internet in an attempt to establish the identity of the users of the jihadist forum.

This scenario poses challenges in that the users of the jihadist websites may include U.S. citizens, foreign intelligence agencies, law enforcement personnel, and researchers in addition to terrorists. Ideally DoD could direct its data collection efforts against just the foreign terrorists, but in reality this is likely impossible and DoD must make a trade-off between over-collecting and under-collecting.

Ethically, this cyber DC is permissible in that it is conducted with the purpose of preventing terrorist attacks, and focused against computers that appear to be in use by terrorists, thereby justifying modest privacy infringements. Under domestic law, this data collection may not be legal depending on the specific techniques used and if some of the affected individuals are U.S. persons. The critical question is if the DC uses methods that constitute an unreasonable search, and thereby require a warrant. As with any intrusion, under the CFAA accessing the websites is illegal for the military to conduct and

only law enforcement and intelligence agencies may conduct this activity. This activity is not limited under international law, and in fact this DC is protected under UDHR 19 as one seeking to receive information. Normatively this action is permissible as long as the techniques used comply with U.S. domestic law.

Operationally, there are a number of considerations to weigh in the conduct of this data collection effort. Strategically, this activity supports the U.S. objective of defeating terrorists, which is a higher order objective than promoting a secure and trusted cyberspace. Executionally, this activity should certainly be conducted clandestinely and covertly. Clandestinely because the detection of the activity by website owners or forum users could force users underground and raise their operational security. Covertly because in conducting collection against the forum users it will be unclear what the intent of the DC effort is, which could be particularly harmful if foreign government agencies are also using the website as a part of their counter-terrorism efforts. Should the DC activity be detected the effect would be communication shifting more secure, or offline, forums with greater security consciousness by users, reducing collection opportunities.

Temporally, to successfully execute this DC effort requires a prior investment into personnel and systems to conduct this activity. While individual actions in this DC operation will take place quickly, conducting a thorough collection will be an operation that takes place over an extended period.


Consequentially, if this DC effort remains undetected there will be no impacts. However, if the activity is detected, but not the U.S. role behind it, there will only be systemic consequences as the demand for more secure communication tools increases. The worst consequences are found if the activity is detected and the U.S. role is determined. To the extent multi-use computer systems were accessed, the U.S. would be subject to domestic and international acquisitions of spying and illegitimate data collection. This may place the U.S. in

the awkward position: if it is unknown the DC operation was a part of counter-terrorism efforts, then the U.S. would have to decide between suffering the operational harm of disclosing the purpose of the operation or enduring the reputational harm while keeping the intent of the operation secret. Such an outrage is bound to decrease U.S. soft power and increase the perception of the U.S. as spying on private citizens worldwide.

Policy Recommendations

- 1) Cyber Data Collection is highly permissible legally, and even has some protection under the UDHR Article 19.
- 2) All DC must be conducted in an effort to protect privacy, both of U.S. persons and foreigners, while achieving higher strategic objectives..
- 3) Privacy expectations and limitations are a currently debated topic. The U.S. should engage in shaping reasonable expectations and norms for privacy protection in cyberspace, as to not overly constrict the legitimate activities of law-abiding nations.
- 4) DC requires continued investment and effort, as the nature of cyberspace evolves so too must DC techniques, tactics, and procedures.
- 5) Substantial care is needed to address operational concerns: cyberspace is an adaptive domain, and the ability to conduct certain DC activities or availability of particular information may disappear as it is collected.

VI. Cyber Attack

Cyber Action	Overall Severity of Implication	Recommendations
Cyber Attack		<ul style="list-style-type: none">• Recognize that Cyber Attacks are a useful, short-of-force, tool for political coercion.• Conduct Cyber Attacks only in a manner that is internationally understood to not constitute an “armed attack.”

Description

External cyber attacks are those external cyber actions with disruptive or damaging effects, logical or physical, of a degree that cannot be reasonably perceived as directly threaten human life. This category includes simple acts of disruption such as distributed denial of service attacks, to physically destructive attacks such as manipulating industrial control systems to destroy, for example, uranium centrifuges. We are differing in our definition of attack from most computer security literature⁸³ to establish an effects-based characterization that is more appropriate for policymaking and more consistent with definitions of attack used in traditional defense and security literature.

Cybersecurity expert Herb Lin has described this category as the most challenging for policy makers saying, “Most cyber actions are in this domain and responding to these actions is by far the most substantial policy challenges in cybersecurity.” This category is the most challenging because external cyber actions rising to the level of a use of force are clearly governed by existing standards regarding the use of force; external cyber actions with consequences

⁸³ In computer security literature an attack is generally defined as an attempt to gain access to a protected computer system or otherwise protected information.

less severe than attack are largely permissible under international law, and even protected in some cases.

Given the complexity of this category, a full analysis requires consideration of intent and deeper situational aspects than the other categories of external cyber we have defined. A full analysis is beyond the scope of this project. Instead, we limit the analysis at present to a general overview of cyber attack, and specific analysis of perhaps the most permissible form of cyber attack—defensive cyber counter-attacks against computer systems presently engaged in conducting a cyber attack.

Policy Analysis

Normative Considerations

Ethical

With the just war tradition⁸⁴ governing use of force and privacy considerations governing non-damaging informational effects, cyber attacks are a category of action that exists in a space with minimal ethical reasoning. Cyber attacks defined as being damaging in nature clearly face a prima facie prohibition. This means the challenge facing cyber policy makers is to establish a rubric for judging when the prima facie prohibition against conducting cyber attacks can be overcome. Depending on the ethical approach taken, one establishes a different set of considerations. Here we consider the consequentialist, deontological, and virtue ethics based approach to this question and what these ethical traditions would identify as the relevant considerations in justifying a cyber attack. Sound cyber policy will have to draw upon and balance each of the ethical considerations identified.

⁸⁴ See for example (Walzer, 1977)

Consequentialist

A consequentialist perspective limits the line of reasoning to a consideration of the likely consequences of the cyber attack. That is that the harm caused by the cyber attack is offset by the good produced. This suggests that cyber attacks whose effects are limited to causing damage to malicious actors are largely justifiable by considering the extent to which they limit these malicious actors from conducting further harm. Cyber attacks against malicious actors are justified as long as they use the minimal amount of force necessary to stop the malicious activity. This is similar to the Just War tradition's principle of necessity – only the minimum level of damage necessary to stop the malicious activity should be used.

For cyber attacks with less narrowly focused effects, it is necessary to consider a balance between harm and good generated. This is similar to the proportionality consideration the department of defense is familiar with considering for governing the use of force. That is, a cyber attack should not cause excessive harm to non-malicious actors relative to the advantage achieved in damaging the malicious actor.

Deontological

The deontological considerations are focused on the duties of the State. The principle ethical duty of the United States is described in the preamble of the Constitution: “*[To] form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity.*” In short, the duty of the U.S. government is to protect the rights and liberty of U.S. citizens and to act in accordance with all U.S. laws (establish Justice). To this we add a second set of duties: to abide by all obligations the U.S. has agreed to through international

treaties. This second set of duties is derived from the U.S. purpose to establish Justice, and its role in respecting international treaties to establish a just international system for U.S. citizens to enjoy.

The strong duties the U.S. government has to U.S. citizens suggest a strongly limited ability to conduct cyber attacks that affect U.S. citizens, but a much more permissive ethical environment for conducting cyber attacks against non-U.S. citizens in order to protect U.S. persons. Any such cyber attack must be conducted while respecting domestic laws and international commitments the U.S. has made.

Virtue

Virtue ethics govern the characteristics of the cyber attacker. The consideration here for cyber policy makers is that in conducting cyber attacks the U.S. government is behaving as a morally good Government would. The U.S. Declaration of Independence identifies the traits a good government possesses (specifically that the State secures for people unalienable human rights (among them life, liberty and the pursuit of happiness) and acts with the consent of the governed). Therefore cyber policy must establish a system that ensures that the U.S. government only conducts cyber attacks that do not endanger inalienable human rights and are conducted with the consent of the governed. Accomplishing this requires effective oversight measures and transparency to ensure U.S. citizens and elected representatives are aware of and consent to the cyber attacks being conducted by the U.S. government.

Domestic Law

As previously noted⁸⁵ the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is a key piece of legislation criminalizing much cyber activity. The CFAA includes particularly strong limitations on causing damage, outlawing in a5:

- (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;*
- (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or*
- (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.*

Section e8 defines damage: “the term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information.”

“Protected computer” includes all computers involved in foreign communication.⁸⁶ The plain language of the CFAA clearly outlaws the conduct of cyber attacks, except when lawfully conducted by law enforcement and intelligence agencies in accordance with paragraph f. These limitations should be corrected by the recommended amendments to the CFAA provided previously in the Cyber Intrusion section.

The second critical domestic legal consideration is that of authorities. Due to the CFAA, all DoD cyber attacks must be conducted under intelligence authorities. This subjects all cyber attacks to the oversight requirements governing intelligence operations and strongly limits the targeting of U.S.

⁸⁵ See section on Cyber Intrusion

⁸⁶ For further discussion see section on Cyber Intrusion

persons. Beyond the limitations placed on all intelligence operations, we identify no additional domestic laws that would govern cyber attacks conducted against non-U.S. persons by intelligence agencies.

International Law

There are few limitations on what we have defined as Cyber Attacks under international law. The UN Charter only limits the “use of force” or conducting “armed attacks” against member states. While we have explicitly defined cyber attack as being less than what could be considered a “use of force,” it is vital to recognize that what constitutes a “use of force” is not well defined or understood. Within the U.S. executive branch, the authority to determine what constitutes a “use of force” rests with the President.⁸⁷ However, internationally it is a matter of customary interpretation. The U.S. should work to establish a clearly understood and agreed upon international interpretation of what constitutes a “use of force,” to avoid misperceptions and potential disproportionate over-reactions to cyber attacks.

Article 5 of the Budapest Convention on Cybercrime requires signatories, “[To] adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.”⁸⁸ In Article 6, it further criminalizes the production or distribution of any device, including computer program, with a primary purpose, which is in violation of Article 5. To the extent this applies to states, this

⁸⁷ See GEN Alexander’s written answers to advanced questions posed by the Senate Armed Services Committee for his nomination hearing on 15 April 2010, available at <http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf>

⁸⁸ (See, Council of Europe, *supra* note 40)

suggests an emergent customary international law against conducting cyber attacks or even acquisition of such capabilities.

The Universal Declaration of Human Rights (UDHR) includes protections against arbitrary attacks on person's property and correspondence.⁸⁹ The UDHR also includes protections for receiving and imparting information, regardless of frontiers, in Article 19. Cyber attacks are by their nature acts of imparting information (typically computer commands), and as such enjoy protection under the UDHR. As long as these computer commands, i.e. cyber attacks, do not arbitrarily deprive people of their property, security, privacy, or correspondence they are permissible under the UDHR, and even protected.

Operational Considerations

Strategic

The U.S. has a strategic interest in a secure and stable cyberspace; conducting cyber attacks clearly undermines this strategic interest. The strategic question, therefore, is what sorts of national interests are of core importance that the U.S. should employ cyber attacks. Using the framework for defining and ranking national interests developed by the commission on America's National Interest⁹⁰ we consider which sort of interests are of sufficient importance to justify employment of cyber attacks.

Vital national interests are of such central importance that the U.S. will go to war to protect them. Certainly cyber attacks – a tool short of war – may be used to protect U.S. vital national interests. And, following the principle military necessity (using the minimal necessary force), the U.S. ought to use cyber attacks

⁸⁹ See Articles 12 and 17 (*See, United Nations, supra* note 44)

⁹⁰ (Allison & Blackwill, 2010)

instead of force, when cyber attacks are likely to be sufficient to successfully protect U.S. vital interests.

Extremely important national interests are those that would severely inhibit the U.S. Government's ability to safeguard and enhance the well being of U.S. citizens in a free and secure nation. Conducting cyber attacks on foreign entities would not have the deleterious effects that would happen should an extremely important national interest be compromised. As such, cyber attacks are strategically permissible to protect extremely important national interests.

Among the U.S.'s important national interests recognized by the commission's report is to "maintain an edge in the

Cyber attacks that promote U.S. vital and extremely important national interests may be appropriate when applied proportionately.

international distribution of information to ensure that American values continue to positively influence the cultures of foreign nations." We assess that the U.S. strategic objective to promote a secure and trustworthy cyberspace⁹¹ to be only of instrumental value for accomplishing this national interest, making it of secondary importance. Consequently, cyber attacks are a strategically appropriate means to protect and achieve U.S. national interests. However, it is clear that some important national interests are undermined in some degree by conducting cyber attacks. For this reason, the conduct of cyber attacks to achieve important national interests requires careful consideration of policy makers, and cyber attacks to protect secondary or lower order national interests require exceptional justification and discrimination in execution.

⁹¹ (See, The White House, *supra* 72)

Executional

At first blush, cyber attacks are highly attractive as a non-lethal, cost-effective means of exerting national influence and securing U.S. national interests. However, cyber-attacks are predicated on the existence of vulnerabilities, including the general vulnerability introduced by simply using computer systems. Operationally it may be in U.S. interests to refrain from using cyber-attacks for all but the most critical purposes in order to prevent potential adversaries from correcting vulnerabilities. However, there exists a mutual dependence on common computer technology; in attempting such a strategy, the U.S. is likely to be leaving itself vulnerable to cyber attacks while the U.S. tries to ensure continued rival vulnerability by refraining to conduct cyber attacks.

Some kinds of cyber attacks that depend on self promulgating viruses also pose challenges in discrimination. Viruses like Stuxnet infected computers in numerous countries worldwide, even if its destructive effects were apparently limited to a very particular configuration of SCADA systems found in Iran.⁹² A key policy challenge is to establish rubrics for measuring and evaluating the disruption caused by the consumed bandwidth, storage, and processor use associated with virus promulgation against the desired effects to ensure such means are appropriately proportionate.

Temporal

Conducting a cyber attack requires prior identification of a rival computer system, its vulnerabilities, access to the targeted system, and the development and testing of an attack method. For the U.S. to conduct cyber attacks at a time and place of its choosing, therefore, requires an ongoing cyber intelligence

⁹² See Symantec's W32.Stuxnet Report. Available at http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

collection effort to generate all this information. This activity is best considered a cyber-specific form of intelligence preparation of the battlefield (IPB) and requires cyber data collection.

Given a cyber attack target and an attack method, the actual execution of a cyber attack can operate at the speed of the access medium – milliseconds for devices connected to the Internet. This ability to rapidly achieve effects makes cyber attacks a potent tool for cyber attackers, and suggests cyber attacks would be some of the first used in an escalating political conflict or war. This rapid attack speed also challenges attacker and victim decision-making processes, which are ill suited for such rapid production of effects.

Consequential

Domestic

The U.S. domestic audience would certainly react negatively to any cyber attacks directed against U.S. persons or close U.S. allies. More generally, there are concerns about cyber attacks as threatening the global common of the Internet, and changing it from a global forum for free communication to one of hostilities and competition. The conducting of cyber attacks by any actor, be it criminal, rival state, or even the U.S, certainly undermines domestic U.S. confidence and trust in cyberspace.

Cyber attacks are also a potentially coercive national tool. A key challenge is establishing effective coordination for the use of cyber attacks among government agencies. Conducting cyber attacks on foreign states or their interests would certainly require input from Department of State. Conducting cyber attacks on U.S. persons would best be overseen by law enforcement authorities, which generally oversee the use of coercive force domestically. Cyber

attacks effecting key sectors such as energy or financial systems would best be conducted with input and oversight from experts in those fields.

International

Foreign States are certain to see cyber attacks against them, their nationals, or against assets located in their country as an infringement of their sovereignty. States are particularly attuned to any such actions conducted by another sovereign power, so that the use of cyber attacks by any state, regardless of the target, incentivizes states to invest in cybersecurity measures. As such it is important for states to reach a common understanding of when cyber attacks are justified. For overt cyber attacks against systems of interest to foreign nationals or against assets located in another sovereign's territory, the U.S. should communicate with the effected states to minimize the perception of an infringement on their sovereignty.

Soft Power

The use of coercive means against any actor is certain to reduce U.S. influence among supporters of that actor. As such, the U.S. should be especially careful in conducting cyber attacks against organizations that enjoy popular support among key audiences. Like using any form of coercion, the U.S. should seek to legitimize the action by using less coercive means first. It should also have declared and generally internationally accepted policies that clearly define when cyber attacks are appropriate. In conducting a cyber attack the U.S. should provide reasonable explanations to the global community of the justice and necessity of U.S. action and how it serves the general good.

Systemic

Anytime computer vulnerabilities are exploited to cause damage or disruption it has two systemic events: increase user awareness of security risks

and incentivize technology companies to correct the vulnerability. Conducting cyber-attacks has the systemic effect of reducing vulnerability to such attacks, according to a senior executive at a Fortune 100 company (who asked not to be identified). The executive commented, “When we learned about Stuxnet our CEO decided to ban the use of USB sticks.” User adaptation is likely the milder systemic effect. The exploitation of computer vulnerabilities increases market demand for secure computer systems, increasing the economic incentives both for computer security firms and for technology developers to invest more heavily in security.

Example Scenario

The following example considers a hypothetical scenario of using cyber attacks to conduct a humanitarian intervention to illustrate the application of the above analytical considerations:

The government of Morundia⁹³ is faced with a domestic political protest. Protests began as peaceful calls for political reform to make the country more democratic, but these protests were harshly repressed with military attacks on the protestors, killing or imprisoning hundreds. The conflict has now escalated to regular artillery shelling on cities and other military actions that are killing hundreds daily.

The U.S. has supported efforts in the UN Security Council to denounce Morundia’s regime and to authorize an intervention to force the country’s regime to allow domestic political reform to proceed. However, a few of Morundia’s allies have promised to veto any such authorization. Under pressure from the U.S. public and Congress to do something, the Executive Branch has been looking to develop options to protect civilians and pressure the Morundian regime to stop their attacks and agree to

⁹³ Morundia is a country long hostile to U.S. interests and has supported attacks against U.S. personnel.

domestic political reforms. One proposed option is to conduct a series of cyber attacks to disrupt military command and control systems to degrade the regimes military capability to conduct attacks and to conduct disruptive information operations to pressure regime leaders to accept political reform, for example by showing senior leaders directly the harm being done to innocent civilians.

This scenario raises the possibility of using cyber attacks as a means to exert coercive influence on a foreign regime short of using force in order to protect civilians. Ethically there is clearly a just cause here; the actions are directed towards protecting innocent life and prevent the killing of civilians. Given that the cyber attacks are directed against a foreign power, there are few limitations under domestic law, as long as the cyber attacks are conducted under proper authorities, with authorization, and with appropriate congressional oversight. To remain legal under international law, it is important that all cyber attacks conducted are tailored to ensure that they cannot be reasonably perceived as an “armed attack” or “use of force” by the targeted country or by other major states. Under the effect test we propose, this means that the attacks cannot be reasonably perceived as potentially lethal. Therefore, we conclude such an attack is normatively permissible.

Considering the operational aspects, this cyber attack seeks to secure U.S. national interests by stopping the large scale taking of human life and encourage political reform in a hostile nation. Compared to other means of military intervention taken in similar situations (such as air strikes or deployment of peacekeepers), cyber attacks provide a low cost and low risk means of intervening. However, conducting cyber attacks will demonstrate U.S. cyber capabilities and the vulnerabilities of command and control systems the U.S. is prepared to exploit. This will lead to a hardening of these systems and degradation in operational capability. The U.S. may want to preserve these

operational capabilities for employment in a situation where higher order national interests are threatened.

Cyber attacks cannot be conducted until key systems and their vulnerabilities are identified. If this has not already been accomplished for Morundia (and particularly its military), targeted cyber attacks will not be possible until this information is collected. Once key systems and vulnerabilities are identified, cyber attacks to exploit them to achieve the desired effects will have to be designed. The U.S. may already have “attack vectors” designed to exploit the types of systems used in the targeted country. Only the “payload” of the cyber attacks would need to be designed, tested, and reviewed, in which case preparation of a cyber attack could take as little as a few weeks. If the U.S. does not already have pre-designed “attack vectors” that will be effective against the targeted country, researching and designing such tools to gain access to targeted cyber systems will delay cyber attacks substantially, on the order of months. Once the decision to conduct the attack is made and the required cyber attack capability exists, effects can be produced very rapidly.

Finally, consider the potential consequences and reactions. Domestically, if the U.S. public is calling for intervention in the targeted country, then conducting cyber attacks is likely to raise few concerns. Some will certainly be considered about the existence of a U.S. capability to conduct such attacks, and some may argue cyberspace should be free of such coercive actions. Others will raise concerns typical to any such operation – that it is not the role of the U.S. government to intervene in any manner in such situations. Internationally, some states will raise concerns that this is an illegitimate infringement on national sovereignty. As long as the nature of the cyber attacks conducted cannot be reasonably construed as an “armed attack,” however, these claims will raise only

moderate concerns; states will also of course internally adapt to limit their exposure to such attacks.

Considering Soft Power, concerns regarding the method of intervention, cyber attacks, are likely to have negligible soft power effects beyond the perceived justice or injustice of intervening. Where intervention is believed to be justified, esteem of the U.S. and U.S. soft power is likely to increase. In addition, the risk of loss of civilian life inherent in military interventions is reduced, thereby minimizing potential negative outcomes. Finally, the systemic effect is certain to be increasing cyber security, as individuals and technology providers adapt to the demonstration of vulnerabilities and the risks they are exposed to in using technology systems. This increased security will benefit the U.S. domestically by reducing vulnerability, even as it degrades U.S. cyber capabilities.


This analysis demonstrates that this decision hangs on the Executorial consideration: will conducting these cyber attacks diminish U.S. ability to employ cyber attacks in situation where higher order national interests are threatened. It is also essential to ensure that the cyber attacks conducted are not perceived as an armed attack in the international system. This requires the establishment of norms and an international understanding of what is a “use of force” in cyberspace.

Policy Recommendations

- 1) To use cyber attacks in the international system the U.S. must establish international norms and understanding on what constitutes an “armed attack” in cyberspace, and ensure all cyber attacks are conducted below the threshold that can reasonably be perceived as an “armed attack” or “use of force.”

- 2) To ensure the operational capability to strike using cyber attacks at a time and place to achieve desired effects, the U.S. Government must be actively identifying potential systems to target and their vulnerabilities, and developing attack delivery vectors.
- 3) CFAA should be amended to allow the military to conduct cyber attacks instead of just intelligence and law enforcement agencies. (See recommendations in Cyber Intrusion section.)
- 4) Increasing transparency and maintaining oversight by elected leaders of all cyber attacks ensures this form of coercion is only applied in situations that U.S. citizens support.
- 5) Cyber attacks are an appropriate means for promoting U.S. vital and extremely important national interests. Cyber attacks may be appropriate, when applied proportionately, to secure important U.S. interests.
- 6) To be consistent with the UDHR and ethical considerations cyber attacks must not arbitrarily deprive people of their property, security, privacy. Cyber attacks should be applied in accordance with principles of proportionality (harm to innocents is proportionate to the advantage gained) and necessity (only the minimally necessary damage to achieve the objective is used).
- 7) A critical effect of conducting cyber attacks is the disclosure of the capability and vulnerabilities exploited. Decision makers need to carefully weigh when to employ cyber attacks. This will likely lead to increased cyber security (which the U.S. will also enjoy) vs. saving this operational capability for later use against a less secure cyberspace.

Cyber Counterattack:

Cyber Action	Overall Severity of Implication	Recommendations
Counterattack		<ul style="list-style-type: none">• Develop matrix to categorize counterattack capabilities based on uniqueness.• Create metrics to categorize scenarios based on imperative to act.• Engage in interagency dialogue to create counterattack norms.• Refine method for executing counterattacks.• Create escalation and de-escalation matrix.

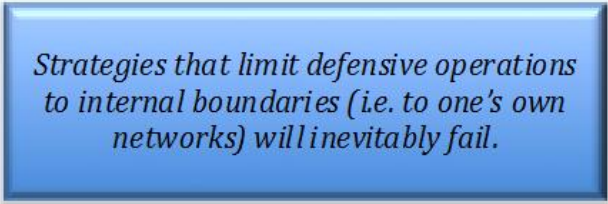
Description

As described in our ontology, cyber counterattack consists of a limited external cyber operation to stop an ongoing hostile external cyber action by affecting the systems involved in the hostile cyber action. Cyber counterattack is a defensive external operation that could be a response to any variety of adversarial external cyber actions, from cyber data collection or DDoS to a cyber attack or cyber force. This is an important distinction, because current literature examining the legality of counterattack has focused on only one aspect of cyber counterattack – the inherent right to self-defense with the use of force based in UN Charter Article 2(4) and Article 51 if the victim of an “armed attack”. Though we will address the legality of cyber counterattack below, it is our assertion that the U.S. should adopt, and be comfortable in other states and actors adopting, a policy of proportionate and discriminate defense in cyberspace, whether the instigating action met the level of “armed attack” or not. Cyber counterattacks would have primarily logical effects and as such do not constitute a use of force

and are entirely permissible ethically and under international law.⁹⁴ Limiting states' and other actors' abilities to defend themselves and their citizens with means that are less than a use of force places undue restrictions on their obligations to protect themselves and their citizens.⁹⁵

There is a second aspect of counterattack as both external and defensive that requires elaboration here, because it is essential to understanding the nature of offensive and defense in cyberspace. As mentioned briefly earlier in the ontology, location of the effects of the operation is a critical aspect of categorizing cyber operations. By location, we do not simply mean geographically (though that is obviously important), but based on ownership or operation of the network. Internal cyber actions occur within a network that an individual, group or organization owns or operates. External cyber actions occur within a network that an individual, group or organization do not own or operate. Defensive operations in cyberspace, however, do not solely remain in internal networks.

Given our experiences with military operations in the physical space, this distinction may cause confusion. It would



Strategies that limit defensive operations to internal boundaries (i.e. to one's own networks) will inevitably fail.

seem counterintuitive that taking the fight to the adversary's "territory" could be defensive. Ground forces protecting a strategic location (e.g. line of communication, high terrain) would designate a perimeter that explicitly distinguishes the area of defense from adversary or neutral territory. A

⁹⁵ Below we will also further examine this aspect, as well as the minimum extent this obligation extends. But it should seem uncontroversial that states have at some basic level the obligation to protect their people and that policies which do so while conforming to international norms of necessity, proportionality and distinction would be unremarkable.

successful counterattack may change the location of the perimeter, but it would seem to defy the definition of “defensive” if the repelling forces took the fight all the way to the attackers’ base of operations. Similarly, in air defense, aircraft may engage with adversary aircraft in the designated engagement zone. Once friendly aircraft had successfully repelled the attackers, it would again strain the definition of “defense” were the defending aircraft to pursue the attackers over hostile territory. In essence, in physical space geographical boundaries play an important role in defining the limits of defensive operations.⁹⁶

The same considerations do not apply for cyberspace, because cyberspace is fundamentally indefensible by establishing location constrained security measures. The attack vectors in cyberspace are virtually infinite, and operators are able to scan for network vulnerabilities at astonishing rates. Simply educating users, maintaining security patches and firewall integrity, and adequately implementing intrusion detection systems (none of which has a 100% success rate) is not sufficient. Yet current cyber policy emphasizes “defensive cyber”, even though it is understood that the current cyber dynamic favors “the offense.”⁹⁷ These conditions remind us of the famous Frederick the Great quote: “In trying to defend everything, he defended nothing.” Strategies that limit defensive operations to internal boundaries (i.e. to one’s own networks) will inevitably fail.

In cyberspace, the only useful defense involves engaging the attacker at the point of origin. Because there are currently no other effective means of defending one’s own network internally, we must recognize that cyber defense

⁹⁶ There is obviously a distinction between defensive operations and armed conflict predicated on individual or collective self-defense.

⁹⁷ One of the more notable attestations to this fact comes from General Hayden’s Black Hat keynote in 2010. http://www.theregister.co.uk/2010/07/29/internet_warfare_keynote/

requires an external component. The most limited and clearly justifiable external defensive component is cyber counterattack.

Policy Analysis

Normative Considerations

Ethical

Ethical considerations for cyber counterattack have two major components: the moral obligation a state owes to the citizens it protects and any moral obligation a state owes to non-citizens that may be affected by the counterattack. The former entails the obligation to protect citizens not only from external threats but also from governmental overreach. The latter depends heavily on the specific ethical framework employed. For this reason, we will mention it superficially, but leave international moral obligations primarily to the international legal section.⁹⁸

Because international moral obligations tend to coincide with international law, we will address it quickly here first. The Lockian conception of the nation state sets the primary responsibility of the state to protect the rights of its citizens. In the case of counterattack it is implicit that the government is responding to an action committed against itself or its people, and therefore the balance of moral obligation to act biases toward protection of the nation's citizens. The parameters of the counterattack, however, must be in accordance with customary law, and we will defer to the international law section for further elaboration.

⁹⁸ Here again we refer to the different aspects of liberalism, particularly cosmopolitanism. Though we have already stated that we will not attempt to justify one specific ethical framework over another, we have left international obligations to the legal section in particular here.

From a domestic perspective, however, it seems almost superfluous to demonstrate to Western audiences the view that governments have a moral obligation to their people. From Kant and Locke to Rawls and Nozick, Western political philosophy has continually espoused the view that governments have a moral obligation to secure and protect the rights of its citizens. Even more specifically to American values, the Declaration of Independence specifically avers that “[g]overnments are instituted among Men” in order to secure their “unalienable rights”. To say that this view is paramount in American political thought is by no means an overstatement

Yet the other side of this obligation is more nuanced. In securing the rights of its people, governments must be wary of breaking them. The balance between security and freedom is a tenuous one, and the potential for eroding basic American rights in the name of cybersecurity is a real hazard. If a foreign-controlled botnet targeting U.S. websites utilizes the computers of thousands of Americans, does the government have an obligation or even the right to remotely disconnect those computers from the Internet? If a foreign government is infiltrating the servers of an American company in order to obtain trade secrets or intellectual property, does the government have the right to monitor the company’s servers without the consent of the victim in order to develop an attributional picture?

The U.S. government should certainly continue to protect the freedoms espoused in the Declaration of Independence and guaranteed through the Constitution, regardless of the cybersecurity threat. To accomplish this, the current gaps in the authorities and capabilities of the U.S. government to protect of private citizens and corporations, need to be corrected. Though we believe that the legal context should evolve to enable better cybersecurity measures, it will be imperative that these measures incorporate robust oversight to preclude

any one branch's overreach. (We have offered suggestions for specific implementation in the recommendation section below.)

Domestic Law

These ethical issues dovetail with the current domestic legal environment, which is hindered in some aspects by a somewhat anachronistic set of rules that cannot sufficiently address the complexity of cybersecurity. To begin, the 4th amendment to the U.S. Constitution offers protection against unreasonable searches and seizures. As mentioned in the framework section, were a foreign-operated botnet to use thousands of U.S. computers to target a U.S. website, the 4th amendment may limit government's response. The Computer Fraud and Abuse Act (CFAA) places prohibitions on accessing a computer without authorization and transmitting code that causes "damage" to that computer. This overly broad legislation criminalizes legitimate actions to protect computer systems under hostile cyber attack.

Even in this introduction to the domestic legality of cyber counterattack, we have been addressing simultaneously two separate issues with a particularly difficult legal dilemma. We are examining the government's protecting its citizens and the way that the government does so. This begs two questions: 1) Who is doing the protecting? and 2) Whom are we protecting? Both questions have specific domestic legal implications. It has been commonly said that CYBERCOM protects .mil websites and DHS protects .gov websites, but that no institution is protecting U.S. .com websites.⁹⁹ Currently there is a legal basis for this. DoD, NSA and DHS cannot monitor domestic networks for a variety of legal reasons. NSA is prohibited from conducting surveillance on U.S. citizens to the point that the "Perfect Citizen" program was met with popular hostility and

⁹⁹ For an example, see (Etzioni, 2011)

skepticism.¹⁰⁰ FISA prevents government electronic surveillance without a FISA court warrant. This is impossible on the large scale required for government to continually protect the private sector networks. It is possible that DoD's protection of citizens using cyber counterattack could be interpreted as a breach of Posse Comitatus.¹⁰¹ Though we believe that government should assume some role of protecting the civilian systems, and have the ability to use cyber counterattacks as required, such a system is currently not feasible under domestic law.

International Law

As mentioned above, the international normative considerations for the use of cyber counterattack concerns international law. Specifically, the Law of Armed Conflict (LOAC) and principles of the Just War tradition requires that any use of force in response to an "armed attack" be necessary, proportional and discrete. The U.S., and any cyber counter-attacker, must adhere to these principles in any form of cyber counterattack, even if the response does not constitute a use of force or the cyber action being responded to has minor effects. The UN Charter only limits states use of force in defending themselves; there is no legal reason U.S. should be limited in its self-defense if the response is not a "use of force" and respects the imperatives of necessity, proportionality and discretion.

At issue with this statement, however, is that there is no appropriate analog to the use of a counterattack that is neither a response to a use of force, nor a use of force itself. For instance, international law has shied away

¹⁰⁰ (Brandon, 2010)

¹⁰¹ One could argue that such a situation would constitute the military's enforcement of domestic law. For one interpretation of this, see (Cavelty, 2008). The actual text of the Posse Comitatus Act can be found here: http://www.dojgov.net/posse_comitatus_act.htm

particularly from limiting espionage¹⁰², and thus there is not necessarily an international legal basis for countering espionage activities. Counterintelligence operations are rooted in domestic law and, whether defensive or offensive¹⁰³, do not correlate to the realm of cybersecurity and the transnational aspects of countering cyber data collection activities.

Operational Considerations

Strategic

There are two main strategic considerations for cyber counterattacks: the relationship between the counterattack and national strategic priorities; and the operational cost/benefit analysis of alerting the attacker that he/she has been identified (and that the U.S. has the technology to stop the attack).

To address the first consideration, we must recognize again the spectrum of cyber operations that the U.S. might want to counter. These incorporate all actions from scanning to cyber force. While DoD may determine that scanning does not threaten the overall strategic goals set forth in the President's National Security Strategy, it is possible that cyber data collection does reach that level. Depending on the type of information targeted, policy-makers may believe that the information collected undermines the ability of the U.S. to prosper. Though somewhat context dependent, these determinations should be determinable ex ante.

The more nuanced scenario includes situations in which a counterattack would alert the attacker to other U.S. operations. For instance, if the U.S. were

¹⁰² In his paper "The Unresolved Equation of Espionage and International Law", Afsheen John Radsan states, "Espionage, filled with paradox and contradiction, continues to have an ambivalent place under international law. To the sophisticated observer, espionage is neither legal nor illegal." See (Radsan, 2007)

¹⁰³ (Counterintelligence)

collecting information from a foreign government, policy-makers may determine that repelling a data collection operation from the same government would have excessively negative repercussions for American operations. If practicable, the U.S. should make value determinations of those operations at the onset of their execution. DoD could rate the strategic value of each cyber operation it conducts and make an associated threshold that must be met before executing a cyber counterattack that would disrupt our own operations. This narrows the uncertainty for policy-makers and decreases response time.

Executional

The primary executional consideration for cyber counterattack centers on the area of responsibility. By that, we must define the actors responsible for doing the countering and the procedural mechanism for conducting the counter. For instance, setting aside all other considerations, if a major U.S. petrochemical company contacts the U.S. government to alert the U.S. Government that the company is the victim of ongoing cyber collection from a foreign source, and are seeking assistance how would the counterattack procedure occur? First, whom does the organization contact (e.g. DHS, NSA)? How do they contact the right entity? What information will be required by the governmental agency? These are only a few of the myriad questions that complicate the operational picture. In this light, the major executional consideration for cyber counterattack is the capability to conduct the operation and having an efficient method used to organize a response.

Another executional consideration will be the issue of escalation. It is possible that a cyber counterattack that meets the requirements of the LOAC will result in a cyber counterattack from the original attacker that is incrementally

more destructive/disruptive. Though DoD has already identified this as a significant complication in the decision making process,¹⁰⁴and mentioned the need for a whole-of-government approach to norm-creation, there has not been discussion about interagency coordination in the executional aspect of cyber counterattack. However, a highly discriminate counter-attack against the offending computer systems that uses the minimally necessary effects to stop the ongoing attack, would minimize the risk of an escalatory cycle.

Additionally, the U.S. must recognize that any use of a cyber operation that produces a knowable and quantifiable impact on an external network risks the possibility of losing the ability to exploit the same vulnerability in the future. For this reason, a counterattack must also consider the cost of lost capability.

As a tertiary tactical concern, the cost of cyber attacks must be considered. If responding to the use of cyber force or other armed attack, the U.S. will have the option to use military forces to respond or to respond with cyber force or attacks. Whether a conventional response would be more cost-effective both immediately and in the long run (e.g. including the cost to find new network vulnerabilities) will be a relevant issue.

Temporal

The speed with which a counterattack needs to be conducted will inevitably affect the decision to use cyber means. Dropping packets against a DDoS or automated hacking back against an identified cyber data collector is generally a quick process. There exists a potential for automated counterattacking capabilities operating at network speeds. Such systems would only require initial policy analysis to ensure the methods they employ are

¹⁰⁴ (Department of Defense, 2011)

discriminate and proportional. The ability to respond to cyber force with a destructive cyber operation is likely not be as immediately executable.¹⁰⁵

Consequential

Domestic

We addressed the nation's legal considerations for effective cyber counterattack operations, but the domestic consequential considerations are much more ingrained in the American psyche. The visceral American distrust of government monitoring is reflected in the law, and this wariness is an impediment to the government's ability to secure cyberspace. A cyber counterattack with a domestic element whether through a citizen's computer or collaboration with a private sector network provider, may create a controversy similar to "warrantless wiretapping."¹⁰⁶

But perhaps the most important domestic consequential issue is the difference in perspective on cyber counterattack between the agencies. Specifically, there are divergent views between the DoD and DoS regarding cyber counterattack. DoS's view is that a cyber counterattack against a foreign individual, group or government entity violates the principle of sovereignty. Though we understand DoS's motivations, we believe that this is a flawed interpretation.¹⁰⁷ Still, the perspective remains and it will be incumbent on DoD

¹⁰⁵ This being an unclassified work, any assumptions on capabilities are highly speculative and hypothetical. For current policy-makers with access, this consideration may very well be knowable beforehand and useful for more robust response scenarios.

¹⁰⁶ (Savage & Risen, 2010)

¹⁰⁷ As we have already mentioned, there is no means of acting in self-defense without employing external cyber operations. It would seem somewhat illogical to emphasize concern for breaking the sovereignty of a foreign nation when there is no recognition that the attacking nation (either through its citizens or government) broke the sovereignty of the United States. This is particularly true in responding to acts of cyber force, but it is also germane to operations with

to reach an interagency understanding on the legitimacy of conducting cyber attacks.

International

The NRC report rightly observes that U.S. cyber operations have the potential to interfere with similar operations of our allied nations.¹⁰⁸ In the event of a cyber counterattack, the U.S. must consider the need to inform allies in the context of the need to respond. Unlike some other forms of external cyber operations (e.g. information collection or cyber force), cyber counterattack, as a defensive action, may have temporal considerations that outweigh the responsibility to alert allies.

As the U.S. considers its policy on cyber counterattack, it must also recognize that it is setting norms. Establishing explicit policy for cyber attacks is challenging due to vagueness in current law including uncertainties in authorities.¹⁰⁹ By developing a responsible cyber counterattack policy, the U.S. will have the advantage of setting the standard to its own purposes and in accordance with its own values.

Soft Power

If properly executed in self-defense, we see no adverse soft power consequences of employing a cyber counterattack. The rationale lies within the natural bias toward defense. In this, there is a distinct second mover legitimacy advantage. In the wake of the 9/11 terrorist attacks, international support for the

predominantly informational objectives and effects. We believe that the ability to use non-destructive, targeted means of countering should mollify DoS's concerns.

¹⁰⁸ (See, National Research Council, *supra* note 20)

¹⁰⁹ Jay P. Kesan and Carol M. Hayes detail a persuasive argument for cyber "counterstriking" (their term) including many of the considerations from our framework. They note, however, that the lack of legal certainty is a significant contributing factor to the current absence of counterattack policy. See (Kesan & Hayes, 2011).

U.S. was very high. But when nations began to believe that the response to the terrorist attacks was not proportionate, discrete, or necessary, they changed their opinions.¹¹⁰ This loss of prestige inevitably had an impact on the U.S.'s soft power.¹¹¹

The key, therefore, for executing a successful cyber counterattack that maintains the U.S.'s soft power will be in ensuring the conditions from the principles of distinction, proportionality, and necessity are met. To demonstrate to the international community that the government response was in line with these principles, the U.S. must be prepared to essentially defend its case. This entails the government's having a series of facts at its disposal: 1) attribution; 2) effect on internal networks; 3) action taken by U.S.; 4) effect on external networks; and 5) measures taken to ensure discrimination, proportionality, and necessity. In some instances, it may be prudent to also have record of post-action diplomatic communiqués to show the importance of dialogue in resolving conflict. All of these actions may require revisiting the classification scheme for U.S. cyber operations in order to better balance the need for operational security with transparency.

Systemic

Though the nature of the Internet favors anonymity, freedom and openness, these same qualities account for a great deal of the insecurity in cyberspace. We believe that there may be a positive systemic effect by creating a norm of cyber counterattack. This is a product of the ability of cyber

¹¹⁰ (Hale, 2002)

¹¹¹ In his book *Soft Power*, Joseph Nye Jr. demonstrated the negative effect of the Iraq War on U.S. soft power, due to the global perception that the U.S. wielded its overwhelming hard power superiority too broadly. See (Nye, Jr., 2004).

counterattacks to serve as a deterrent. Much has already been written about the need to create a deterrence strategy in cyberspace.¹¹²

As noted above, there are many ways to achieve deterrence,¹¹³ but having a credible response that erodes the benefit of committing the offending action is an important method. A U.S. policy of cyber counterattack will alter the way individuals interact with the Internet – but in a way that makes it more secure.

Example Scenario

To synthesize the considerations detailed extensively above, consider the following scenario:

A major U.S. technology company, Lycast, has identified suspicious traffic within its servers. Upon further investigation, Lycast recognized that successful spear-phishing campaigns have used a zero-day exploit in Internet Explorer to gain access to the company's sensitive systems. Lycast had initiated a trace back and found that intellectual property and other protected data was exfiltrated to an IP address located within the U.S. The company has determined that the U.S. IP address is continually sending data to a server located in Gendia. Gendia is a country with which the U.S. has normalized relations and significant economic integration. Lycast has alerted their contacts in DoD,¹¹⁴ and they have requested assistance.

DoD has identified the server in Gendia, recognized that there are significant amounts of data being received at the particular IP address, and confirmed with Lycast

¹¹² Perhaps the most exhaustive study of cyber deterrence is Martin Libicki's report through the Rand Corporation for the U.S. Air Force. See (Libicki, 2009).

¹¹³ For specific applicability to cyberspace, see Joseph Nye's "Nuclear Lessons for Cyber Security?" (Nye, Jr., Nuclear Lessons for Cyber Security?, 2011)

¹¹⁴ For simplicity's sake in this scenario, we are postulating that the appropriate agency for the company to contact is DoD. Whether policy-makers choose to assign cyber counterattack responsibility to another agency (perhaps DHS), the considerations we have addressed remain. What is important here is the fact that the private institution has contacted the U.S. government, a facet to which we will return at the end of the scenario.

the identity of the IP address in question. Additionally, DoD has the ability to target the computer in Gendia and have the computer shut down, and it believes there will be little to no collateral damage should DoD choose to execute a counterattack. Lycast has told DoD that should the government not act, they will respond on their own accord.

This scenario is modeled off the Google Aurora attacks,¹¹⁵ with the addition of a domestic complication. As reported, Google took the initiative to hack back in order to gather information about the attack.¹¹⁶ Yet neither Google nor the U.S. government chose to execute a cyber counterattack. Given the scenario above (even with the extra dimension), we believe that the U.S. could have employed a cyber counterattack in accordance with our framework.

Normatively, we have stated that the U.S. government has the obligation to protect its citizens.¹¹⁷ This is clearly an instance of a tort, as defined within U.S. law, committed against a U.S. company. We believe that the government has an ethical obligation to respond, as it would should Lycast contact their local law enforcement regarding a physical break in at their headquarters.

The domestic legal aspect of this is more complicated, because Lycast sees that the Gendian hackers are using a co-opted American computer as an intermediary. By U.S. law, the government has limited options to monitor the American computer without a FISA court warrant.¹¹⁸ Obtaining the warrant,

¹¹⁵ (Operation Aurora)

¹¹⁶ (Sanger & Markoff, 2010)

¹¹⁷ Though beyond the scope of this analysis, corporate personhood confers the rights of a person to U.S. corporations. We raise it here to simply demonstrate that the government's obligation to protect its people would extend to corporations through the transitive property of equality. See (Corporate personhood).

¹¹⁸ In emergency situations, the Attorney General can authorize immediate surveillance, though it is uncertain if the Attorney General would believe this is such a case. See (United States Foreign Intelligence Surveillance Court).

however, may require a significant amount of time, and the government may have a limited window in which to act. First, Lyncast has indicated that they will take action to prevent further loss if DoD does not act. Second, DoD has an opportunity to act while the Gendian hackers are in the process of exfiltrating data. Should they stop, the necessity condition may not be achievable because there is no ongoing hostile cyber action. It is possible that the government could employ the same attack to shut down the computer within the U.S., but that may also pose a 4th Amendment dilemma if the action constitutes an unreasonable search or seizure.

Internationally, the LOAC applies and DoD believes that it can meet the conditions of proportionality and discretion. We argue that the requirement for necessity exists, because of the ethical obligation to protect U.S. citizens. As described above, we believe other international legal aspects are too vague to categorically prohibit a cyber counterattack.

Internationally, there are no legal constraints in responding with means that do not constitute a use of force. However, the principles of discrimination, proportionality, and necessity should still be followed. That is to say the counterattack should target only the attacking systems and avoid any collateral harm, should be proportionate in the harm prevented to any incidental harm caused by the counterattack, and generate only the minimum necessary disruption or damage to stop the hostile action.

Strategically, the cyber counterattack is in line with the administration's National Security Strategy tenants of security and prosperity. In fact, an October 2011 Office of National Counterintelligence Report specifically states: "Foreign

economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security."¹¹⁹

Operationally, the government has the ability to conduct the counterattack, and there is no indication that the technology used to stop the Gendian computer from exfiltrating data is particularly unique or immediately perishable. Were the counterattack capability sensitive, however, it would further complicate matters. Policy-makers would have to assess whether the loss of capability is worth repelling the attack. This condition, however, is context dependent and we cannot make a categorical determination here.

The greatest operational implication for a cyber counterattack is the risk of escalation. DoD does not know what the Gendian reaction would be to the counterattack. It is possible that the Gendian government may not recognize that the counterattack had occurred or who conducted it. Additionally, it is possible (if not probable) that the Gendian government does not have an escalation matrix or even policy for responding to a cyber counterattack.

Consequentially, the greatest difficulty with conducting a cyber counterattack here is the interagency implication. For instance, assuming that the Gendian government would attempt to categorize the counterattack as a blatant demonstration of U.S. aggression, this poses serious complications for DoS in maintaining normalized diplomatic relations. We have already illuminated the issue of sovereignty (and our beliefs of its applicability), but DoS's concerns can be mitigated through prior coordination. Additionally, a well-articulated policy *ex ante* that warns nation states and individual actors of U.S. intentions to conduct cyber counterattacks could preempt criticism *ex post*.

¹¹⁹ (Office of the National Counterintelligence Executive, 2011)

There is a possibility of a backlash in the international community that could erode U.S. soft power, though a policy of transparency regarding the operation might dampen this type of negative response. As noted above, it will be important to ensure the counterattack is discriminate, proportionate, and causes the minimal necessary disruption. The U.S. should maintain records to demonstrate that its response was justified to potential critics. Additionally, the U.S. could aver that it believes all nations have the same right to act as the U.S. has done in order to allay concerns of the U.S.'s assuming a role of cyber hegemon. Framing here will be critical.

Though a cyber counterattack will inevitably result in international implications for relations between the U.S. and Gendia, we see no significant complication with other nations. This is the case should the U.S. government decide to conduct the operation itself. Lycast has indicated that it will take action should the government choose not to. It is unclear what the reaction would be should a private institution assume the responsibility to conduct cyber counterattacks, it may deflect criticism from the U.S. Government or be a destabilizing trend leading to private firms externally responding in self defense.

Policy Recommendations

Cyber counterattack is a legitimate and important aspect of cybersecurity. For that reason, we recommend that DoD pursue the following:

- 1) Establish a declaratory policy: "The United States reserves the right to protect its citizens and defend U.S. interests in cyberspace from foreign action, using all appropriate mechanisms while respecting domestic and international law."
- 2) Promote as an international norm that victims of hostile cyber actions conduct discriminate, proportionate, and necessary limited cyber


- counterattacks to stop ongoing hostile action. Reform laws, such as the CFAA, to allow for this.
- 3) A matrix to categorize DoD counterattack capabilities based on uniqueness (i.e. its value) and effect (from minor to informational to destructive). This matrix can be applied to specific scenarios in order to facilitate compliance with the requirements of proportionality and discretion.
 - 4) A spectrum that categorizes scenarios based on imperative to act (from none to conditional to high). This spectrum can be used to facilitate compliance with the requirement of necessity.
 - 5) Interagency dialogue regarding the intent of DoD to establish a collaborative process to execute counterattacks. Such a dialogue should address the issues described above in order to analyze impediments, both legitimate and constructed, that may limit the effectiveness of these operations.
 - 6) A procedure for initiating and conducting cyber counterattacks. This would include identifying one agency private companies should contact in the event of their becoming victims of a cyber attack, as well as a response plan for coordinating with other relevant agents in government.
 - 7) An escalation and de-escalation matrix in the event of a cyber counter-attack to prevent dangerous escalatory cycles. Strategically and consequentially, the U.S. would have greater success in de-escalating and seeking a coordinated response through the international community.

Conditions that have to be present for the use of cyber counterattack:

- 1) Use of cyber counterattack must conform to the principles of proportionality, necessity, and distinction. If these factors cannot be assured, cyber counterattack is not the correct policy.

- 2) The foreign external cyber operation must pose a significant threat to the American people such that the continued operation would undermine the country's strategic goals. This suggests that only foreign external cyber operations that have substantial effects meet the appropriate threshold.

VII. Cyber Force

Cyber Action	Overall Severity of Implication	Recommendations
Cyber Force		<ul style="list-style-type: none"> • Do not engage in cyber force unless the following conditions are met: <ul style="list-style-type: none"> ○ Conforming to LOAC ○ Minor or no spillover effects (if overt) ○ Coordinated with allied partners and legitimized through multi-national body ○ In concert with traditional military force and as targeted as possible ○ Limit use of catastrophic cyber force to situations of declared general warfare.

Description

As described in our ontology, cyber force includes cyber attacks with such substantial physical effects that they rise to a level that ought to be considered a “use of force” under international law. Although the general international norms of use of force stem from the UN Charter Article 2(4), the actual bounds of “force” are nebulous.¹²⁰ This is true not only for cyber operations, but has also been true for physical ones in which the concept of “I know it when I see it”¹²¹ has become predominant. In his 2002 paper “Information Warfare and International Law on the Use of Force”, Jason Barkham suggests that the definition of “force” must change in order to accommodate new technologies in information warfare (IW).¹²² As of this writing, however, there have been no such clarifying distinctions.

¹²⁰ (Hoisington, 2009)

¹²¹ (Jacobellis v. Ohio, 1964)

¹²² Barkham argues that either the application of Article 2(4) must change or the international community must develop a new standard, possibly through treaties. See (Barkham, 2002)

For the purpose of this work, a precise definition of “use of force” is not required, but only recognition of the criteria for determining what qualifies a use of force. To avoid questions of means and target sets that make applying cyber operations to the traditional definitions of “use of force” difficult, we have focused on the effect of the an operation as the most appropriate metric to judge if something is a “use of force.” If a cyber operation were to result in physical injury or death such that conventional means of achieving the same ends would be considered a “use of force,” then the cyber operation is “cyber force.” Similarly, if the cyber capability can be employed in a manner that could be reasonably perceived as intent to cause physical injury or death similar to effects caused by traditional kinetic weapons, then this cyber operation is “cyber force”. In this regard, therefore, we have limited this definition to cyber attacks with the potential for direct lethal effects.

This description may seem to lack nuance, but our intention is to provide clarity for policy-makers who may otherwise feel paralyzed by the technical aspects of cyberspace or the difficulty in applying traditional military conceptual frameworks to cyber operations. For this reason, it is our contention that the main driver for policy-makers should not be the specific means of the operation,¹²³ but rather the effect that that operation produces.¹²⁴ Also, it is

¹²³ In “Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities”, the National Academy of Sciences offers the example of blockade and sanctions to describe the way means, not effects, differentiates a use of force from an action which does not meet that criteria. It is an important distinction for consideration, but one that does not apply here. In our conceptualization, the appropriate analogy for cyber force is not with blockade or sanctions, but with conventional weapon type. (See, National Research Council, *supra* note 20)

¹²⁴ An appropriate example would be the contention that lines of code in and of themselves are not weapons, and thus a destructive operation that solely relies on the use of code could not reach the threshold of “use of force”. This is an erroneous assertion. It is precisely the code in Joint Direct Attack Munitions (JDAM) that makes it effective, requiring the military to use less payload and resulting in smaller circular errors of probability (CEP). As a function of payload required to technology available (i.e. computer code), we can identify that the more technology

important to note that in discussing cyber force, we are focusing on the specific execution of code that directly resulted in the effects constituting a use of force. We do not broaden this definition to include supporting cyber operations (such as cyber information collection) that may enable DoD's use of cyber force.

In that regard, the following analysis of cyber force requires the policy-maker to conceptualize the external cyber operation as

We anticipate that any use of cyber force, especially outside the context of declared hostilities, would have negative strategic implications..

essentially equivalent to a conventional operation that has effects that would be considered a use of force. From this vantage point, it will become obvious that the majority of the considerations from our framework for cyber force correspond to the same considerations for conventional uses of force.

Policy Analysis

Normative Considerations

Ethical

Ethical considerations for cyber force mirror those for conventional operations that are considered use of force. Just war theory and particularly the concepts of *jus ad bellum* and *jus in bello* apply. With regard to cyber force, as a type of weapon, there should be no ethical distinction between the use of cyber force and any other type of attack that results in effects commensurate with the use of force.

available, the less payload is required for any given level of effect. Thus, it is arguable that cyber force represents the logical conclusion to a capability of zero payload required for the same effect, because of greater technology available.

Although the ethical considerations are the same, the ability to meet those standards may be more difficult in cyber force. The requirements for distinction, proportionality and attribution, as noted above, are problematic in cyberspace. When considering the use of cyber force, policy-makers should emphasize the possibility of collateral damage from unforeseen spillover due to network connectivity. In 2003, it is reported the U.S. chose not to conduct cyber attacks on Iraqi banks because of their connection connection to French financial networks. It was feared an errant cyber weapon might disrupt ATM service in Europe.¹²⁵ We recommend that policy-makers continue to bias toward prudence in order to ensure the primacy of these ethical considerations.

This bias would have implications for the rare (though not inconceivable) use of cyber force against American citizens residing outside the U.S. who had become involved in terrorist plots against the U.S. The recent killing of U.S. citizen Anwar Al-Awlaki in Yemen for his ties to Al Qaeda in the Arabian Peninsula (AQAP) demonstrates this issue.¹²⁶ Were the method for the killing cyber force instead of a drone strike, the ethical (and in fact legal) issues remain the same. Here the considerations of ethics, law and soft power overlap. Not only does the U.S. hold strong convictions regarding the principle of “guilty until proven innocent” as guaranteed by the constitution, but the effect of such force on the attractiveness of the U.S. abroad also has consequences on American soft power. This is not to pass judgment on the Al-Awlaki killing as an extension of counterterrorism operations, but it is a relevant analogy for U.S. use of cyber force. We believe that policy-makers should prioritize the ethical and legal

¹²⁵ (Smith, 2003)

¹²⁶ For a general overview of the legal debate regarding the Al-Awlaki killing see (Williams C. J., 2011)

dimensions in their decision making for the greater strategic and soft power aims.

Domestic Law

The domestic legal considerations for cyber force are limited, because cyber force is essentially an external operation directed at other nation states or non-state actors. And because we have limited our definition of cyber force to the proximal cause of the force, domestic law concerning the citizenry has little applicability (aside from the issue raised above under ethical considerations). Questions of privacy, surveillance or seizure are generally not relevant.

The issue of Title 10 and Title 50 authority, however, does apply here as a consideration for the assets used to conduct the cyber force. Because resident expertise resides within DoD, the CIA and the NSA, the context will most likely dictate the best assets to execute the operation if policy-makers decide to use cyber force. Here, domestic law overlaps with strategy. Policy-makers' strategic imperatives may dictate which domestic legal considerations exist, and these considerations themselves may influence the strategy that policy-makers pursue.

International Law

The bulk of the normative considerations for the use of cyber force rests in international law. This constellation of customary law, treaties and base law encompass the Law of Armed Conflict (LOAC) and are particularly relevant to cyber force. Despite this fact, LOAC remains the same for cyber force as it does for the use of force in conventional methods. When considering any use of force (cyber or otherwise) policy-makers will undoubtedly consider LOAC as well as Article 3 of the Universal Declaration of Human Rights, which guarantees the

right to “life, liberty and security of person”.¹²⁷ In this regard, cyber force is an unambiguous case of the applicability of international law to external cyber operations. For this reason, it requires no elaboration here.

Operational Considerations

Strategic

Operational considerations mark the beginning of separation between cyber force and more conventional uses of force and strategic considerations remain paramount in this aspect. The major distinction between these uses of force is the fact that cyber force is unprecedented. Despite some speculation to the contrary,¹²⁸ there is no historical example of a nation-state or non-state actor using cyber technology to produce effects equivalent to conventional use of force. Even the Stuxnet virus, by our definition, would not be considered cyber force, because the effect of intervening with centrifuge operations does not reach the force threshold.

This fact is a critical strategic concern, because the first use of cyber force may have greater strategic implications that extend beyond the scope of the operation itself. Context here, though, is critical. Using cyber force as a force multiplier of conventional weapons during declared hostilities and against a well-defined adversary could be analogous to the use of stealth technology in Panama or Gulf War I. It would simply serve as the first example of new defense technology. Conversely, the covert use of cyber force or even the use of cyber force during asymmetrical or low intensity conflict may prove less acceptable.

¹²⁷ (See, United Nations, *supra* note 44)

¹²⁸ As an example, a former Air Force secretary has claimed that the U.S. had created faulty code that the Soviets used in 1982 in a gas pipeline, which caused a massive explosion rivaled only by a nuclear detonation. See (Loney, 2004)

Especially with the rise in power of the traditionally powerless,¹²⁹ policy-makers must think beyond a realist, sovereign nation, international relations model and anticipate the strategic consequences of using cyber force from an individual level. Considering the democratizing power of the Internet and cyberspace, we would anticipate that any use of cyber force, especially those not used in conjunction with conventional forces in declared hostilities, would have negative strategic implications. This could manifest itself simply as loss of domestic support from the electorate, retaliation from hacktivist groups such as Anonymous, and/or significant adverse response abroad.

From a theater strategy perspective, we believe that the authority to use cyber force should, like all other forms of force, rest with the President of the United States. In his essay “Ten Propositions Regarding Cyberspace Operations”, Major General Williams argues that the Joint Forces Commander (JFC) should have command and control over cyberspace within his domain similar to the control he has of the terrestrial domain.¹³⁰ Due to the unprecedented nature of cyber force, delegating authority to the JFC for the use of cyber force would be a mistake. While General Williams argues that operations in cyberspace are akin to those in the terrestrial domain, the possibility of collateral damage outside of the JFC’s area of responsibility (AOR) with cyber capabilities makes them substantially different. Some limited cyber capabilities may be appropriate at the JFC level, but not those that may have effects extending beyond their AOR. Had CENTCOM chosen to use cyber attacks in Iraq in 2003 and its use had severed banking communications in France, the political and strategic implications

¹²⁹ For a thorough discussion on the rise of the traditionally powerless and the conditions that have precipitated this change in power dynamic, see (Kellerman, 2008).

¹³⁰ (See, Williams B. T., *supra* note 32)

would be hard to overstate.¹³¹ This is a key example of theater strategy gravely affecting national strategy.

This analysis does not necessarily suggest that the U.S. should adopt a blanket no first use policy for cyber force. However compelling arguments may be for a declared no first use policy for nuclear weapons,¹³² there is no such imperative here. Unlike cyber force, nuclear weapons have very little gradation of effect – it is always catastrophic. Use of a nuclear weapon escalates a conflict to general war. Using cyber force may be possible in the context of limited war. It is possible that a very targeted, well-contained first use of cyber force would be an excellent policy choice normatively, operationally and consequentially. The burden of proof, however, for such a claim, considering the strategic implications noted above, would be exceptionally high.

Executional

Regarding cyber force, the primary Executional consideration will be the potential loss of the vulnerability that enabled its use in the first place. As mentioned in the framework discussion, cyber weapons are unlike conventional weapons in that the use of a cyber weapon may mean that its capability for future use vanishes. This fact is true for any external cyber operation, but it is particularly relevant here, because the effects of cyber force reveal the nature of the attack. The adversary would attempt to remedy the vulnerability and the international computing community would almost certainly work to analyze and decode the cyber force payload.¹³³ Thus, policy-makers must weigh the

¹³¹ This is particularly true in light of the fact that France, and most of Western Europe, was already opposed to Operation Iraqi Freedom.

¹³² For instance, see (Gerson, 2010).

¹³³ This was in fact exactly the result of the Stuxnet virus. Network security experts have thoroughly analyzed its code by leveraging bulletin boards and various resources on the Internet.

operational benefits of employing cyber force with the cost of losing the capability. Does the operational situation merit the use of a particular cyber force? Does using cyber force offer more valuable information to the adversary about U.S. capability, such that its use would become an operational error?

As a secondary Executional concern, the cost of a cyber force must be considered. While the use of cyber technology may be more cost-effective in many aspects of external cyber operations, it is not clear that that is the case for cyber force. The actual execution of code may be minimal, but the time required to design, gather intelligence, monitor adversary networks, test capabilities, etc. may be extremely costly. Cyber capabilities at the level of cyber force are not ubiquitous, nor are they easily achieved. As will be demonstrated in the next section, cyber force is not necessarily the quickest solution (regardless of the speed of code execution). For this reason, it may not be the most efficient. This work is not an exercise in defense budgeting, but the way in which DoD costs its weaponry will affect the weapon's attractiveness as a cost-effective solution. Especially when considering the weapon on a cost per total use basis, cyber force may not be the ideal solution.

Temporal

As alluded to in the previous section, cyber weaponry may not necessarily work in milliseconds when analyzed in context. This is particularly true for cyber force, because the capability often requires extensive planning and preparation. If speed is a key component in determining the appropriate method of employing force, cyber may not be the best option.

Though certain aspects of the code remain highly encrypted (and making attribution exceedingly difficult), its use in current form may now be very limited. For an overview of the history of decoding Stuxnet, (See, Zetter, *supra* note 8)
For a technical analysis, see Symantec's dossier (Falliere, Murchu, & Chien, 2011).

Consequential

Domestic

As mentioned in the domestic legal consideration section, cyber force is predominantly internationally focused. The object of the operation should not be a U.S. citizen or his property and certainly not one within the U.S. itself. For that reason, domestic political consequences center mostly on interagency and inter-branch issues.

The first incorporates the different interests among U.S. agencies, interests (and vantage points) that may not seem complimentary. These differences self-evidently originate from distinct missions and concepts of public value. Regarding cyber force, DoD may find an imperative to act that DoS (for instance) does not see. Yet any execution of cyber force by DoD will inevitably have implications for other agencies and their missions. With the case of DoS, their diplomatic endeavors may suffer. While we will examine the potential effect of cyber force on U.S. international relations in a subsequent section, it is important to note here that other agencies have a vested interest in any use of force, particularly one that is relatively new and poorly understood. The federal government has rightly endeavored to align the different agencies' efforts for a more holistic approach, and it is imperative for DoD to support these initiatives.

Because the use of force has damaging effects, the implications of such operations for other agencies are even more pronounced. DoS seeks ensure the safety of U.S. citizens who live abroad, whether for diplomatic, educational, leisure or business reasons. They must have statements prepared for their host nations and for diplomats in the U.S. who might request further insight into the U.S. operation. Treasury may be concerned about the effect a destabilizing event might have on U.S. economic outlook. Homeland Security may raise the threat

level domestically to protect against any immediate retaliation at home. The CIA may be inclined to prioritize assets on intelligence collection at the locus of the cyber operation in order to gauge the effectiveness of the operation or the local response to it.

These are mundane examples of the competing interests among agencies. What is critical here, however, is that **cyber force as not simply a use of force, but a new form of an armed attack, imposes uncertainty onto other agencies, markets, and the public.** To mitigate any potential destabilization of this uncertainty, DoD must liaise with other agencies in preparation of the use of cyber force. Here, domestic political overlaps with temporal considerations. This may be a time-consuming process and one that may not suit operational requirements. Were there to be adequate channels to facilitate such dialogue and/or a unified concept of cyber force among the agencies, this might mitigate the temporal dilemma. Regardless, the decision to use cyber force will inevitably require coordination across agencies and Presidential authorization.

The second aspect of domestic political considerations that are particularly germane to cyber force is the role of Congress and the interaction between the legislative and executive branches. The issue of Title 10 vs. Title 50 authority will determine oversight requirements for cyber operations,¹³⁴ but the use of force itself may be constrained constitutionally. The constitution rests the power to declare and fund war with the legislature, though it places the responsibility of foreign policy on the executive. The War Powers Resolution has attempted to clarify that relationship, although virtually every president has claimed that the legislation infringes on the executives authority.¹³⁵ At issue here, therefore, is the

¹³⁴ (Chesney, 2011)

¹³⁵ (Library of Congress, 2011)

extent to which the executive branch may use cyber force without declared hostilities. As using cyber force doesn't require the deploying of military forces, it may create a dilemma for congressional oversight. Ensuring proper authorization and a real need to use force may require new legislation.

International

The NRC report rightly observes that U.S. cyber operations have the potential to interfere with similar operations of our allied nations.¹³⁶ When considering the damaging effects of cyber force, the U.S. should liaise with allied nations to discuss possible conflict with their cyber operations. There are myriad ways in which U.S. cyber operations could affect those of our allies, but what is critical here is the recognition that, particularly with cyber force, the U.S. should deconflict with friendly nations operating on the systems the U.S. plans to exploit.

Also, because cyberspace is a rapidly developing domain, there is great potential for norm-setting. Psychologically, there are various reasons for conforming to a particular conduct, and unanimity of action is one of the more potent methods of strengthening conformity.¹³⁷ Thus, it would benefit the U.S. to support the conduct it would wish to become the norm. That is, if the U.S. has an interest, as it likely does, in restricting the use of cyber force internationally, then it should seek to adhere to this standard.

Soft Power

Over the past decade, hard power has dominated U.S. foreign policy often to the detriment of U.S. influence and national security. To avoid such missteps

¹³⁶ (See, National Research Council, *supra* note 20)

¹³⁷ Over time, individuals internalize the norm, making it the most powerful determinant in conformity. For a brief overview, see (Williams R. , 1992)

in cyberspace, policy-makers should analyze the way the international community will interpret American use of cyber force. While this may seem self-evident, especially in light of the fact that we have often equated cyber force with other uses of force, there are relevant distinctions for force executed through cyberspace.

First, the history of cyberspace (and particularly the Internet) has overwhelmingly been driven by non-military use. The inherent insecurity with current global networks stems predominantly from the fact that the Internet was originally designed for openness and flexibility.¹³⁸ Security has always been a secondary concern. For this reason, the overwhelming majority of users of cyberspace place a premium on the nature of the Internet as an open, empowering medium. Use of cyber force may alter foreign perception of the U.S. as trying to militarize cyberspace. The Chinese have already asserted that, by creating CYBERCOM, the U.S. has indeed done exactly that.¹³⁹ An actual use of cyber force might convince others that the Chinese argument has merit.

For that reason, cyber force, as the sole aspect of an operation, may be counterproductive to U.S. interests if the destructive effect were large enough, if there were significant collateral damage, or if the targets were non-state actors. Drone strikes against Tehrik-i-Talibani (TTP) in the tribal areas of Pakistan are contentious enough (and certainly have a cost in terms of U.S. soft power). Targeting any insurgent or terrorist group through cyber means may prove even more costly.

As described in the “Strategic” section above, cyber force as an aspect of a coordinated (and legitimized) military operation may appear to the international

¹³⁸ (Froehlich & Kent, 1998)

¹³⁹ (Segal, 2011)

public as new U.S. military technology and not civilian technology co-opted by the world's remaining hegemon for military purposes. This is a critical distinction, and the context of using cyber force may drive the way it is perceived abroad and hence the way such an operation affects American soft power.

Systemic

Systemic implications for cyber force have the potential to be significant. From one perspective, an actual, documented use of cyber force is a powerful motivator for cyberspace. While current discussions of cybersecurity are often technical, hypothetical and dramatic – many times to the point of seeming alarmist – the image of a destroyed electrical power station could change the way society perceives connectivity.

In a positive way, individuals may recognize the need for greater personal involvement in promoting cybersecurity. Private industry and entrepreneurs may identify for-profit services (above and beyond current offerings) that emphasize securing networks. Administrators and non-governmental bodies may have greater success in addressing systemic issues with the current networking structures in cyberspace (such as IPv4, and border gateway protocol (BGP) and domain name server (DNS) vulnerabilities). In much the same way that the September 11th terrorist attacks changed the way Americans perceive security, an actual act of cyber force may have the same impact.

Yet an act of cyber force may have a completely different effect. The current nature of cyberspace is determined as much by norms and perceptions as it is by the laws of code. Companies have been employing the technologies of connectivity for great social surplus, whether through online banking, e-commerce, or electric smart grids. How such companies may react should they find themselves operating in a newly perceived “battlespace” is unknown.

Would the threat of cyber force limit businesses' investment in network connectivity? Perhaps the threat of being targeted may make transactions more costly and force businesses to alter the way they operate in cyberspace. This has not been the case for other, less destructive forms of cyber operations. But as mentioned multiple times before, cyber force is unprecedented.

Though many of the other considerations in our framework are common (and applicable) to other forms of military force, systemic considerations are entirely new. Consequently, they are very hard to predict. But it is imperative for policy-makers to recognize that in the developing medium of cyberspace, significant actions have serious, literally paradigm-shifting, consequences.

Example Scenario

To synthesize the considerations detailed extensively above, consider the following scenario:

In support of overseas contingency operations (OCO), the United States intelligence community (IC) has successfully located a high value target (HVT) in a major city in Ardia. Ardia is a country with which the U.S. has normalized relations, but whose population has very low approval ratings of the U.S. The HVT assists in financing a major terrorist organization, and is known to have funneled over \$250M from donors around the globe to various arms of the organization. Through SIGINT and HUMINT, the IC believes they have located the HVT in a specific apartment complex where he has amassed a series of computers to support international crime and his laundering activities.

DoD is aware of a vulnerability in a particular personal computer that allows the attacker to control the battery management microprocessor to make the battery explode.¹⁴⁰

¹⁴⁰ (Sutter, 2011)

IC believes that the HVT is using 3 of these computers in his “control room” and DoD believes that they can exploit the vulnerability to engage the target. Because of the size of the batteries, DoD estimates that there would be little to no fragmentation effects in neighboring apartments, though the HVT would probably be eliminated.

Determining whether DoD should contact the cyber operation, we can again use our framework. Though lethal targeting of a foreign national suspected of supporting terrorist organizations may be ethically questionable, we can cede this point based on precedent.¹⁴¹ Legally, the executive could justify such force through the AUMF and the inherent right to self-defense (which it has done in the past as well). The case under international law is more problematic, as the executive would still have to ensure necessity, proportionality and distinction. In fact, it is unknown whether the HVT is the sole user of the computers. He does live with his wife and three children, though the IC claims that they are aware when the HVT is alone in the apartment.

Operationally this cyber operation appears to support the overall strategic goal of disrupting the terrorist organization. There are, however, very serious questions about the relations between Ardia and the U.S. and whether targeting an individual within its sovereign territory is best for the two countries' relations. Also, America has a greater strategic objective of stability within the region that may be harmed by the operation. Operationally, this exploit is well known and its use does not necessarily prevent its future use, nor is it a more significantly developed exploit. Temporally, cyber force would be a good option, because the HVT has no set pattern of being in his apartment and a quick strike would be required. Also, the exploit is currently available and waiting.

¹⁴¹ We have already raised the example of drone strikes on known or suspected insurgents or terrorists.

Though the strategic consideration for the operation is troubling, consequential factors bring even greater uncertainty. The American people are overwhelmingly in favor of such strikes, because they do not put troops in harm's way. There is also broad support within Congress for supporting counterterrorism operations. Regarding soft power, however, this operation becomes less appealing. Polls in Ardia and within the region show that targeted killings of suspected terrorists have eroded American influence. It is becoming increasingly more difficult for Ardian politicians to support American priorities, even when they are in line with Ardian aims. Allied nations in the West have condemned American use of targeted killings. If the cyber force were in fact to harm one of the HVT's family members instead of the HVT, this would have profound implications for U.S. soft power abroad. It is also unknown how our allies would react to killing through the suspected terrorist's computers, vice through purely military means. Currently, DoD is unaware of any other allied operations concerning this particular HVT. DoD is leery to share this data as the U.S. has been searching for this HVT for many years. This would also be the first use of cyber force and the international implications are unclear. Lastly, the effect of using cyber force on the nature of the Internet is unknown. It is possible that this type of operation is limited enough in scope to have minimal effect.

In such a situation, our recommendation would be to refrain from using cyber force for primarily ethical and consequential reasons. First, we believe that the use of force in cyberspace, as a new and unique medium, requires biasing toward prudence. Without a clear ability to determine distinction, the U.S. would fail to uphold the LOAC. This in turn may have serious implications for U.S. strategy in the region as well as for U.S. relations with Western allies.

Policy Recommendations

- 1) Use of cyber force must conform to all laws governing the use of force. In particular cyber force must conform to the LOAC, especially regarding proportionality and distinction, and the UN Charter. If these factors cannot be assured, cyber force is not the correct weapon.
- 2) If overt, cyber force should be limited in scope with assurance that any operation has minor if any spillover effects.
- 3) Cyber force should be coordinated with our allied partners and perhaps legitimized through a multi-national body (NATO at least, U.N. if possible or required).
- 4) Cyber force should be in concert with traditional military force and as targeted as possible.
- 5) Catastrophic (i.e. expansive and destructive) use of cyber force should only be considered for retaliatory measures or in conjunction with prolonged, declared, large-scale hostilities.
- 6) The President should set a declaratory policy that clearly defines what constitutes a use of force and relate this to cyber force. We recommend the following effects based statement, “Any action in cyberspace which directly place at risk the life of U.S. citizens constitutes an armed attack against the U.S, and will be responded to at a time, place, and manner of our choosing in accordance with domestic and international law.”

VIII. Conclusion

As the nature of war changes with technological advancement, societies and militaries are compelled to adapt to effectively compete in the new environment. The dawn of the Information Age has created the new, unique, man-made domain of cyberspace, challenging policy makers to determine how the U.S. government should engage in this domain. Recent events have shown that cyberspace is a critical environment for the U.S. and much of the world, and it therefore can be the vector for coercive cyber attacks. For this reason, there is a clear role for the U.S. Government in engaging in this domain to protect national interests from malicious actors.

To aid policy makers in establishing effective and appropriate cyber policy, this project developed a new effects-based ontology for describing cyber actions in a policy relevant manner. This ontology gives policy makers a tool that provides meaningful and readily determinable distinctions between various cyber activities, free from the uncertainties and meaningless distinctions of existing frameworks predicated on the actor or the intent. Using this ontology we have identified twelve key categories of external cyber operations relevant to policy makers that are being discussed today.

Conducting policy analysis in cybersecurity, requires a comprehensive framework that does not exclude any key considerations. Towards, this end we developed a ten aspect analytical framework that examines the Normative, Operational, and Consequential considerations of cyber actions. This framework provides policy makers a starting point for conducting a comprehensive evaluation of a cyber action in order to establish effective and appropriate policy. To demonstrate the use of this framework we analyzed six critical categories

identified by our ontology, spanning the spectrum of effect intensity caused by external cyber action.

Our analysis has produced a number of specific recommendations for DoD in resolving key policy issues concerning external cyber operations. These recommendations are summarized in Appendix 1. However, there also exist larger questions regarding the role of government in cyberspace not directly addressed in the preceding discussion.

As noted in the Cyber Attack section, much of cyber activity exists in an effects-space that does not threaten human life and cannot be properly considered “force,” in the classic political science sense. Political scientists from Hobbes through Weber have defined the role of the state as maintaining a monopoly on the legitimate use of force. In engaging with the policy challenges associated with cyberspace, policy makers and legislators need to be careful to not move too quickly and establish policies or rules that place inappropriate constraints on actions, as we believe is the case with legislation like the CFAA and DMCA, or to establish an overly expansive role for government.

Big questions have not been addressed in our project, and answering them may not be possible at this time. Questions like: Should the government have a monopoly on the use of external cyber actions? Can the government have a monopoly on it? What sorts of external cyber actions are permissible for the private sector to execute? How intolerable are various cyber actions? What is an appropriate investment to deter these actions? To what extent should the U.S. degrade its external cyber capabilities in order to create a more secure cyberspace?

It is likely too early to answer these questions until the nature of conflict in cyberspace is better developed and citizens developed refined perspectives on government’s role in cyberspace. Until these questions are closer to being settled,

it is important that policy makers do not overly constrain U.S. options in cyberspace, either through policy or law, and instead maintain robust capabilities and engage in extensive stakeholder dialogue to create a cyberspace that is aligned with American values.

We hope policy makers find the analysis presented in the project of external cyber action useful in conceptualizing the relevant distinctions in cyber activity and that it better prepares them for the important work of shaping U.S. policy in cyberspace. We encourage humility in addressing cyber policy challenges. American values and identification of American interests in cyberspace are still developing; as they develop the most important thing for the U.S. policy makers is to reduce acute vulnerabilities and remain adaptive.

Appendix 1: Summary of Recommendations

Scanning

Scanning presents no ethical or substantial legal concerns; however, it does pose some political and operational issues. As such, it should be conducted with some policy oversight to:

- 1) Establish an interagency understanding that scanning is a part of good modern cyber intelligence practice and due to its benign nature should be minimally constrained.
- 2) Avoid exaggerated policy rhetoric that describes scanning as attacks. While this is accurate in computer security parlance, it is highly confusing in the policy debate and greatly exaggerates the threat faced.
- 3) Encourage good trade practice in conducting of external scanning activities. Operationally try to avoid scanning of systems owned by U.S. persons, but recognize that such collection is permissible.
- 4) Have a process to share identified vulnerability operation with the owner of the vulnerable system when appropriate. This will require some declassification and consideration of operational impacts, but also setting up a politically acceptable information sharing process. Recommend conducting any information sharing through DHS law enforcement agencies.
- 5) Responding to cyber scanning is principally an operational intel gain/lose consideration, it is not a policy concern. Taking external action beyond scanning or efforts to determine the origin in response to scanning is ill-advised. Better to analysis the information provided by being scanned to prepare defensively.

Intrusion

- 1) Intrusions should only be conducted when they can be expected to improve the security of cyberspace or in support of a higher order U.S. Strategic objective.
- 2) Policy oversight is required to determine when the U.S. is best served in disclosing an identified computer vulnerability to try and correct it, and when it is best to keep the vulnerability secret for future exploitation.
- 3) The CFAA needs to be amended, while remaining consistent with the Budapest Convention on Cybercrime, to clarify who the statute applies to and narrow the scope of what is outlawed to only that which is objectionable. Specifically we recommend the following amendments:
 - a. Protection for foreign computers needs to be weakened. The definition of protected computer, (e)(2)(b), should be changed to “which affects the operation of critical infrastructure important to the United States, including public utilities, communication systems, financial institutions, and public safety systems, even if that computer is located outside the United States.
 - b. Criminalizing computer access “without authorization”¹⁴² cedes too much authority to private actors, allowing them to criminalize action through Terms of Service (TOS). Statute should instead criminalize only the circumvention of a security measure; amend (a)(2) to “Intentionally circumvents a security measure to accesses a computer, without authorization or exceeds authorized access, and thereby obtains —”

¹⁴² 18 U.S.C. § 1030 (a)(2)

- c. Amended (a)(2) (a), (b), and (c) by replacing “information” with “protected private information.” Where private means that information which is not publically available and protected meaning the holder of the information has made positive steps to prevent the information from being publically known.
 - d. Section (f) should be expanded to exempt the lawfully authorized activities of the U.S. Military and Department of Homeland Security from prohibition.
- 4) Customary international law on cyber-intrusions is emerging. U.S. should work to set a norm that is not overly restrictive. An overly restrictive international legal standard would bind the legitimate actions of law-abiding nations and increase the vulnerability to rogue actors.
- 5) Consider signaling dynamics in intrusions; when possible signal the limited scope of an intrusion to avoid the risk of escalatory cycles.
 - a. Similarly, be careful in responding to detected intrusions to avoid over-reaction.

Data Collection

- 1) Cyber Data Collection is highly permissible, and even has some protection under the UDHR Article 19.
- 2) All DC must be conducted in an effort to protect privacy, both of U.S. persons and foreigners.
- 3) Privacy expectations and limitations are a currently debated topic. The U.S. should engage in shaping reasonable expectations and norms for privacy protections, as to not overly constrict the legitimate activities of law abiding nations.
- 4) DC requires continued investment and effort, as the nature of cyberspace evolves so too must DC techniques, tactics, and procedures.

- 5) Substantial care is needed to address operational concerns: cyberspace is an adaptive domain, ability to conduct certain DC activities or availability of particular information may disappear, may disappear as it is collected upon.

Cyber Attack

- 1) To use cyber attacks in the international system the U.S. must establish international norms and understanding on what constitutes an “armed attack” in cyberspace, and ensure all cyber attacks are conducted below the threshold that can reasonably be perceived as an “armed attack” or “use of force.”
- 2) To ensure the operational capability to strike using cyber attacks at a time and place to achieve desired effects, the U.S. must be actively identifying potential systems to target and their vulnerabilities, and developing attack delivery vectors.
- 3) CFAA should be amended to allow the military to conduct cyber attacks instead of just intelligence and law enforcement agencies, see recommendations in Cyber Intrusion section.
- 4) Increasing transparency and maintaining oversight by elected leaders of all cyber attacks ensures this form of coercion is only applied in situations that U.S. citizens support.
- 5) Cyber Attacks are an appropriate means for promoting U.S. vital and extremely important national interests. Cyber attacks may be appropriate, when applied proportionately, to secure important U.S. interests.
- 6) To be consistent with the UDHR and ethical considerations cyber attacks must not arbitrarily deprive people of their property, security, privacy. Cyber attacks should be applied in accordance with principles of proportionality (harm to innocents is proportionate to the advantage

gained) and necessity (only the minimally necessary damage to achieve the objective is used).

- 7) A critical effect of conducting cyber attacks is the disclosure of the capability and vulnerabilities exploited. Decision makers need to carefully weigh when to employ cyber attacks. This will likely lead to increased cyber security (which the U.S. will also enjoy) vs. saving this operational capability for later use against a less secure cyberspace.

Counterattack

We believe that cyber counterattack is a legitimate and important aspect of cybersecurity. For that reason, we recommend that DoD pursue the following:

- 1) Establish a declaratory policy: “The United States reserves the right to protect its citizens and defend U.S. interests in cyberspace from foreign action, using all appropriate mechanisms while respecting domestic and international law.”
- 2) Promote as an international norm that victims of hostile cyber actions conduct discriminate, proportionate, and necessary limited cyber counterattacks to stop ongoing hostile action. Reform laws, such as the CFAA, to allow for this.
- 3) A matrix to categorize DoD counterattack capabilities based on uniqueness (i.e. its value) and effect (from minor to informational to destructive). This matrix can be applied to specific scenarios in order to facilitate compliance with the requirements of proportionality and discretion.
- 4) A spectrum that categorizes scenarios based on imperative to act (from none to conditional to high). This spectrum can be used to facilitate compliance with the requirement of necessity.

- 5) Interagency dialogue regarding the intent of DoD to establish cyber counterattack as policy and to establish a collaborative process to execute counterattacks. Such a dialogue should address the issues described above in order to analyze impediments, both legitimate and constructed, that may limit the effectiveness of these operations.
- 6) A procedure for initiating and conducting cyber counterattacks. This would include identifying one agency private companies should contact in the event of their becoming victims of a cyber attack, as well as a response plan for coordinating with other relevant agents in government.
- 7) An escalation and de-escalation matrix in the event of a cyber counter-attack to prevent dangerous escalatory cycles. Strategically and consequentially, the U.S. would have greater success in de-escalating and seeking a coordinated response through the international community.

Conditions that have to be present for the use of cyber counterattack:

- 1) Use of cyber counterattack must conform to the principles of proportionality, necessity, and distinction. If these factors cannot be assured, cyber counterattack is not the correct policy.
- 2) The foreign external cyber operation must pose a significant threat to the American people such that the continued operation would undermine the country's strategic goals. This suggests that only foreign external cyber operations that have substantial effects.

Cyber Force

- 1) Use of cyber force must conform to all laws governing the use of force. In particular the LOAC, especially regarding proportionality and distinction, and the UN Charter. If these factors cannot be assured, cyber force is not the correct weapon.

- 2) If overt, cyber force should be limited in scope with assurance that any operation has minor if any spillover effects.
- 3) Cyber force should be coordinated with our allied partners and perhaps legitimized through a multi-national body (NATO at least, U.N. if possible or required).
- 4) Cyber force should be in concert with traditional military force and as targeted as possible.
- 5) Catastrophic (i.e. expansive and destructive) use of cyber force should only be considered for retaliatory measures or in conjunction with prolonged, declared, large-scale hostilities.
- 6) The President should set a declaratory policy that clearly defines what constitutes a use of force and relate this to cyber force. We recommend the following effects based statement, "Any action in cyberspace which directly place at risk the life of U.S. citizens constitutes an armed attack against the U.S, and will be responded to at a time, place, and manner of our choosing in accordance with domestic and international law."

Appendix 2: Glossary

Cyber Action: the subset of cyber activity which produces logical or physical effects beyond that which is generally found or intended during normal operation computer systems.

Cyber Activity: All activity conducted through cyberspace.

Cyber Attack: External cyber actions with disruptive or damaging logical or physical effects. Cyber attack can be conducted for offensive, defensive, or informational objectives.

Cyber Counterattack: limited External cyber operation directed just to stop an ongoing use of offensive cyber action; for example, by stopping an ongoing cyber attack by affecting the participating computer systems.

Cyber Force: Cyber attacks with such substantial effects that they should be considered a “use of force” or “armed attack” under international law.

Cyber Data Collection: External cyber actions with no substantial disruptive or destructive effect, but access of protected data. Protected data is all data not authorized for access or normally accessible to general users.

Cyber Denial of Service: Disrupting access to information services without disrupting the confidentiality or integrity of the data, or destroying any systems. Such attacks are commonly conducted by botnets in a distributed denial of service attack (DDoS).

Cyber Information Dissemination: External cyber action which disseminates protected information to a non-privileged audience with no substantial direct disruptive or destructive effects. For example, Wikileaks publically posting classified documents.

Cyber Intrusion: Unauthorized access of a computer system or access which exceeds authorization.

Cyber Operations: The subset of external or internal cyber actions which are conducted to achieve a specific objective.

Cyber Pre-emption: External cyber operation to prevent an anticipated hostile cyber action. For example conducting a botnet take down.

Cyber Retaliation: External cyber operation to impose costs on an actor for aggressive actions. Cyber Retaliation could be a tool to establish deterrence in international relations short of using force.

Cyber Sabotage: Cyber attacks which cause the physical destruction of equipment or systems, without directly endangering human life, typically accomplished through giving improper commands to industrial control systems. Stuxnet was a cyber sabotage attack.

Cyber Scanning: The unauthorized testing, probing, or scanning of a computer system to search for potential vulnerabilities.

Cyberspace: A global domain consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Defensive objectives: Objectives seeking to secure one's own systems or preserve freedom of operation.

External cyber action: Cyber actions with effects on systems not owned or operated by the actor.

Informational Objectives: Objectives seeking to access or impart information. Such objectives receive some protection under UDHR Article 19.

Internal cyber action: Cyber actions with effects only on systems owned or operated by the actor.

Logical effects: Effects on data, accessibility, and information within cyberspace with minimal physical manifestations. All cyber actions have logical effects.

Military cyber operations: Cyber operations where the objective is military in nature.

Offensive objectives: Objectives which are intended to coerce rival action, impose costs, or degrade rival capabilities.

Physical effects: Those effects which are tangibly observable by people; only some cyber operations have physical effects, for example those affecting the logic in control systems.

Bibliography

- Allison, G. T., & Blackwill, R. (2010). *America's National Interests*. Harvard Kennedy School of Government, Belfer Center for Science and International Affairs. Cambridge: Harvard University Press.
- Ambrose, S. E. (1984). *Eisenhower The President* (Vol. II). New York, NY, U.S.A.: Simon & Schuster.
- Barkham, J. (2002). Information Warfare and International Law on the Use of Force. *New York University Journal of Law and Politics* , 34, 57-113.
- BBC News. (2010, October 18). *Cyber attacks and terrorism head threats facing UK*. Retrieved January 10, 2012, from [bbc.co.uk](http://www.bbc.co.uk/news/uk-11562969):
<http://www.bbc.co.uk/news/uk-11562969>
- BBC News. (2011, November 11). *EU austerity drive country by country*. Retrieved January 10, 2012, from [bbc.co.uk](http://www.bbc.co.uk/news/10162176): <http://www.bbc.co.uk/news/10162176>
- Bloomfield, R. E., Gashi, I., Povyakalo, A. A., & Stankovic, V. (2008). *Comparison of Empirical Data from Two Honeynets and a Distributed Honeypot Network*. City University London, City Research Online. London: Centre for Software Reliability.
- Bradbury, S. G. (2011, March 4). The Developing Legal Framework for Defensive and Offensive Cyber Operations. *Harvard National Security Journal*.
- Brandon, J. (2010, July 13). *Is the NSA's 'Perfect Citizen' the Ultimate Spying Tool?* Retrieved February 1, 2012, from [foxnews.com](http://www.foxnews.com/scitech/2010/07/13/nsa-perfect-citizen-ultimate-spying-tool/):
<http://www.foxnews.com/scitech/2010/07/13/nsa-perfect-citizen-ultimate-spying-tool/>

- Brito, J., & Watkins, T. (2012). Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy. *Harvard National Security Journal* , 3 (1), 39-84.
- Cavelty, M. D. (2008). *US efforts to secure the information age*. New York, NY, U.S.A.: Routledge.
- Chesney, R. (2011, December 14). *Offensive Cyberspace Operations, the NDAA, and the Title 10 - Title 50 Debate*. Retrieved January 28, 2012, from Lawfare: <http://www.lawfareblog.com/2011/12/cyberoperations/>
- Clarke, R.A. and Knake, R.K. (2010). *Cyber war: The Next Threat To National Security And What To Do About It*. New York, NY, U.S.A: HarperCollins Publishers.
- Collins, S. (2011, March 7). *Hot to Make Internet More Secure*. Retrieved January 5, 2012, from politico.com: <http://www.politico.com/news/stories/0311/50742.html>
- Corporate personhood*. (n.d.). Retrieved February 13, 2012, from Wikipedia.org: http://en.wikipedia.org/wiki/Corporate_personhood
- Council of Europe. (2001, November 23). Convention on Cybercrime. Budapest, Hungary.
- Counterintelligence*. (n.d.). Retrieved February 12, 2012, from Wikipedia.org: <http://en.wikipedia.org/wiki/Counterintelligence>
- Department of Defense. (2011). *Cyberspace Policy Report*.
- Electronic Frontier Foundation. (2010, February 12). *Computer Fraud and Abuse Act (CFAA) - Internet Law Treatise*. Retrieved January 7, 2012, from ilt.eff.org: [http://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_\(CFAA\)](http://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA))

- Etzioni, A. (2011). Cybersecurity in the Private Sector. *Issues in Science and Technology* , Fall, 58-62.
- European Commission. (2011, June 16). Europeas share data online, but privacy concerns remain. Brussels, Belgium.
- Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier*. Symantec, Security Response.
- Froehlich, F. E., & Kent, A. (1998). *The Froelich/Kent Encyclopedia of Telecommunications* (1 ed., Vol. 15). New York, NY, U.S.A.: CRC Press.
- Gabriel, R. A., & Metz, K. S. (1992, June 30). *The World's First Armies*. Retrieved February 1, 2012, from A Short History of War:
<http://www.au.af.mil/au/awc/awcgate/gabrmetz/gabr0004.htm>
- Gerson, M. S. (2010). No First Use: The Next Step for U.S. Nuclear Policy. *International Security* , 35 (2), 7-47.
- Global Security. (n.d.). *Aviation History*. Retrieved Febuary 1, 2012, from [globalsecurity.org:
http://www.globalsecurity.org/military/world/china/aviation-history-1.htm](http://www.globalsecurity.org/military/world/china/aviation-history-1.htm)
- Goldsmith, J. L., & Wu, T. (2007). *Who Controls the Internet? Illusions of a Borderless World*. Oxford Univeristy Press.
- Gourley, B. (2008, May 29). Towards a Cyber Deterrent. Retrieved November 20, 2011, from Social Science Research Network:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1542565
- Greenemeier, L. (2011, June 13). The Fog of Cyberwar: What Are the Rules of Engagement? *Scientific American*.

Hale, E. (2002, August 14). Global warmth for U.S. after 9/11 turns to frost. *USA Today* .

Hersh, J. (2011, October 16). Egyptian Activists See Hypocrisy in BART Shutdown, London Riots. *The Huffington Post* .

History of the Internet. (n.d.). Retrieved February 20, 2012, from Wikipedia.org:
http://en.wikipedia.org/wiki/History_of_the_Internet

History of the World. (n.d.). Retrieved February 20, 2012, from Wikipedia.org:
http://en.wikipedia.org/wiki/History_of_the_world

Hobbes, T. (1985). *Leviathan*. London, UK: Penguin.

Hoisington, M. (2009). Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. *Boston College International and Comparative Law Review* , 32 (2), 439-454.

Hosenball, M. (2012, January 12). *Lawmakers press Homeland Security on Internet monitoring*. Retrieved January 15, 2012, from reuters.com:
<http://www.reuters.com/article/2012/01/13/us-usa-security-internet-idUSTRE80C06T20120113>

Infoplease. (n.d.). *Computer Virus Timeline*. Retrieved February 1, 2012, from Infoplease.com: <http://www.infoplease.com/ipa/A0872842.html>

International Humanitarian Law Research. (2009, June). *IHL Primer #1 - What is IHL?* (H. University, Producer) Retrieved January 5, 2012, from ihl.ihlresearch.org:
<http://ihl.ihlresearch.org/index.cfm?fuseaction=page.viewpage&pageid=2083>

Internet Systems Consortium. (2012, January). *The ISC Domain Survey*. Retrieved February 1, 2012, from [isc.org](http://www.isc.org/solutions/survey): <http://www.isc.org/solutions/survey>

- Jacobellis v. Ohio, 11 (United States Supreme Court June 22, 1964).
- James, M. (2011, April 19). *U.S. Authorities Pull the Plug on Major Botnet, 2 Million Zombie PCs Rejoice (Sort Of)*. Retrieved January 15, 2012, from allspammedup.com: <http://www.allspammedup.com/2011/04/u-s-authorities-pull-the-plug-on-major-botnet-2-million-zombie-pcs-rejoice-sort-of/>
- Kellerman, B. (2008). *Follwership, How Follwers Are Creating Change and Changing Leaders*. Cambridge, MA, U.S.A.: Harvard Business School Press.
- Kesan, J. P., & Hayes, C. M. (2011, April 7). Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. *Harvard Journal of Law and Technology*.
- Kish, J. (1995). *International Law and Espionage*. (D. Turns, Ed.) The Hague, The Netherlands: Kluwer Law International.
- Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York, N.Y., U.S.A.: Basic Books.
- Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Rand Corporation.
- Library of Congress. (2011, April 4). *War Powers*. Retrieved January 30, 2012, from loc.gov: <http://loc.gov/law/help/war-powers.php>
- Lin, H. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy* , 4 (1), 63-86.
- Linder, D. (2012). *The Right of Privacy: Is it Protected by the Constitution?* Retrieved January 5, 2012, from Exploring Constitutional Conflicts: <http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html>
- Loney, M. (2004, March 1). *US software 'blew up Russian gas pipeline'*. Retrieved February 2, 2012, from ZDNet: <http://www.zdnet.co.uk/news/it-strategy/2004/03/01/us-software-blew-up-russian-gas-pipeline-39147917/>

- Lynn, W., & Cartwright, J. (2011, July 14). Defense Strategy for Operating in Cyberspace.
- McConnell, M. (2010, February 28). How to Win the Cyberwar We're Losing. *The Washington Post*.
- McConnell, M., Chertoff, M., & Lynn, W. (2012, January 27). China's Cyber Theivery is National Policy - And Must Be Challenged. *The Wall Street Journal*.
- Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*.
- Moulton v. VC3, 1:00-CV-434-TWT (United States District Court Northern District of Georgia November 6, 2000).
- Nakashima, E. (2011, July 14). U.S. cyber approach 'too predictable' for one top general. *The Washington Post*.
- National Research Council. (2010). *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC, U.S.A.: National Academies Press.
- National Research Council. (2009). *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. (W. A. Owens, K. W. Dam, & H. S. Lin, Eds.) Washington, D.C., U.S.A.: National Academies Press.
- Naval Warfare*. (n.d.). Retrieved February 1, 2012, from Wikipedia:
http://en.wikipedia.org/wiki/Naval_warfare#History
- Nicaragua v. United States of America, (International Court of Justice June 27, 1986)
- Nye, Jr., J. S. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*, 5 (4), 18-38.

- Nye, Jr., J. S. (2004). *Soft Power*. New York, NY, U.S.A.: PublicAffairs.
- Office of the National Counterintelligence Executive. (2011). *Foreign Spies Stealing US Economic Secrets in Cyberspace*.
- Operation Aurora*. (n.d.). Retrieved February 15, 2012, from Wikipedia.org:
http://en.wikipedia.org/wiki/Operation_Aurora
- Radsan, A. J. (2007). The Unresolved Equation of Espionage and International Law. *Michigan Journal of International Law* , 28, 595-623.
- Roscini, M. (2010). World Wide Warfare - Jus ad bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law* , 14, 85-130.
- Sanger, D. E., & Markoff, J. (2010, January 14). After Google's Stand on China, U.S. Treads Lightly. *The New York Times*.
- Savage, C., & Risen, J. (2010, March 31). Federal Judge Finds N.S.A. Wiretaps Were Illegal. *The New York Times*.
- Schmitt, E. , & Shanker, T. (2011, October 18). U.S. Debated Cyberwarfare Against Libya. *The New York Times*.
- Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *The Columbia Journal of Transnational Law* , 37, 885-937.
- Scramjet*. (n.d.). Retrieved February 20, 2012, from Wikipedia.org:
<http://en.wikipedia.org/wiki/Scramjet>
- Segal, A. (2011, December 27). *Ideas about China's Cyber Command*. Retrieved January 17, 2012, from Council on Foreign Relations:
<http://blogs.cfr.org/asia/2011/12/27/ideas-about-chinas-cyber-command/>
- Shanker, T. (2011, October 18). U.S. Weighs Its Strategy on Warfare in Cyberspace. *The New York Times*.

- Slade, R. M. (1992). *History of Computer Viruses*. Retrieved February 1, 2012, from Doug's Home on the Web: <http://www.dmath.org/virus/papers/history-of-computer-viruses.html#C06>
- Smith, C. R. (2003, March 13). U.S. Information Warriors Wrestle With New Weapons. *Newsmax.com*.
- Sutter, J. D. (2011, August 5). *Hacker can shut down Apple MacBook battery*. Retrieved February 3, 2012, from cnn.com: http://articles.cnn.com/2011-08-05/tech/miller.apple.battery.hacks_1_passwords-battery-apple-security?_s=PM:TECH
- Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society* , 31 (1).
- The White House. (2012). *Consumer Data Privacy in a Networked World*.
- The White House. (2009). *Cyberspace Policy Review*.
- The White House. (2011). *International Strategy for Cyberspace*.
- The White House. (2010, May). *National Security Strategy 2010*.
- Torture Memos*. (n.d.). Retrieved November 20, 2011, from Wikipedia.org: http://en.wikipedia.org/wiki/Torture_Memos
- U.S. Joint Chiefs of Staff. (2012). *Joint Publication 1-2: Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C., U.S.A.: Department of Defense.
- U.S. Joint Chiefs of Staff. (2006). *Joint Publication 3-13: Information Operations*. Washington, D.C.: Department of Defense.
- United Nations. (1945, June 26). *Charter of the United Nations*. San Francisco, CA, U.S.A.

United Nations. (1948, December 10). Universal Declaration of Human Rights. New York, NY, U.S.A.

ICTY: *About the ICTY*. (n.d.). Retrieved December 20, 2011, from icty.org:

<http://www.icty.org/sections/AbouttheICTY>

United States Foreign Intelligence Surveillance Court. (n.d.). Retrieved February 12, 2012, from Wikipedia.org:

http://en.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court

United States v. Jones, 10-1259 (Supreme Court of the United States January 23, 2012).

US-CERT. (n.d.). *Control Systems - Cyber Threat Source Descriptions*. Retrieved

January 6, 2012, from us-cert.gov: http://www.us-cert.gov/control_systems/csthreats.html

Walzer, M. (1977). *Just and Unjust Wars: A Moral Argument*. New York, NY, U.S.A.: Basic Books.

Weber, M. (1919, January). Politics as a Vocation. Munich, Germany.

Williams, B. T. (2011). Ten Propositions regarding Cyberspace Operations. *Joint Forces Quarterly*, 2nd quarter (61), 10-17.

Williams, C. J. (2011, September 30). Awlaki death rekindles debate on targeting Americans. *The Los Angeles Times*.

Williams, R. (1992). *Lecture 05 - Social Psych: Conformity*. Retrieved January 17, 2012, from nd.edu:

<http://www.nd.edu/~rwilliam/xsoc530/conformity.html>

Wolf, J. (2011, October 18). *U.S. crafting framework for cyber offense: general*.

Retrieved January 15, 2012, from reuters.com:

<http://www.reuters.com/article/2011/10/18/us-usa-cyber-warfare-idUSTRE79H6B520111018>

Zetter, K. (2011, July 11). *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*. Retrieved February 1, 2012, from Wired.com: <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1>

Zittrain, J. (2009). *The future of the Internet and How to Stop It*. New Haven, CT, U.S.A.: Yale University Press.

