Calhoun: The NPS Institutional Archive

Theses and Dissertations | Thesis Collection

2014-03

Attribution, delayed attribution and covert cyber-attack. Under what conditions should the United States publicly acknowledge responsibility for cyber operations?

McDade, Wylie

Monterey, California: Naval Postgraduate School

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ATTRIBUTION, DELAYED ATTRIBUTION AND COVERT CYBER-ATTACK. UNDER WHAT CONDITIONS SHOULD THE UNITED STATES PUBLICLY ACKNOWLEDGE RESPONSIBILITY FOR CYBER OPERATIONS?

by

Wylie McDade

March 2014

Thesis Co-Advisors: Wade Huntley
Dorothy E. Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
ATTRIBUTION, DELAYED ATTRIBUTION AND COVERT CYBER-ATTACK. UNDER WHAT CONDITIONS SHOULD THE UNITED STATES PUBLICLY ACKNOWLEDGE RESPONSIBILITY FOR CYBER OPERATIONS?

5. FUNDING NUMBERS

6. AUTHOR(S) Wylie McDade

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Self-attribution is a public declaration of responsibility for the conduct of an operation. It is distinguished from covert operations, where perpetrators provide no such acknowledgement and attempt to conceal their identities. Although self-attribution is always an option, this thesis examines legal and strategic reasons for a nation state to publically acknowledge its role in the conduct of a cyber-operation. The central result is that whereas neither international law nor national policy requires self-attribution, under certain strategic conditions it may be preferred.

14. SUBJECT TERMS: Self-attribution, public acknowledgement, cyberattack

15. NUMBER OF PAGES
83

16. PRICE CODE

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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ATTRIBUTION, DELAYED ATTRIBUTION AND COVERT CYBER-ATTACK. UNDER WHAT CONDITIONS SHOULD THE UNITED STATES PUBLICLY ACKNOWLEDGE RESPONSIBILITY FOR CYBER OPERATIONS?

Wylie McDade
Lieutenant, United States Navy
B.A., The George Washington University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2014

Author: Wylie McDade

Approved by: Wade Huntley
Thesis Co-Advisor

Dorothy E. Denning
Thesis Co-Advisor

Cynthia Irvine
Chair, Department of Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Self-attribution is a public declaration of responsibility for the conduct of an operation. It is distinguished from covert operations, where perpetrators provide no such acknowledgement and attempt to conceal their identities. Although self-attribution is always an option, this thesis examines legal and strategic reasons for a nation state to publically acknowledge its role in the conduct of a cyber-operation. The central result is that whereas neither international law nor national policy requires self-attribution, under certain strategic conditions it may be preferred.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C-CXA	Combined Cyber Exercise Area
CG-NAT	Carrier-Grade Network Address Translation
CNCI	Comprehensive National Cybersecurity Initiative
CRKI	critical resources key infrastructure
CXA	Cyber Exercise Area
DDoS	distributed denial of service
DoD	Department of Defense
HSPD-7	Homeland Security Presidential Directive
IP	Internet Protocol
ISP	internet service provider
J-CXA	Joint Cyber Exercise Area
LOAC	Law of Armed Conflict
MAC	media access control
NSS	National Security Strategy
USCYBERCOM	United States Cyber Command
US-ISC	United States International Strategy for Cyberspace

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The cipher and the key are attributed to BLAISE just in case you are bored on watch…

Usiak mnalm qiupl myeoe dwmfm
ptzsr taoaa xjznz wuvtr mkev
yiymi lpy.B zeuve gdmfd vzsx
zuzsp mteaoi spMIF RJYGC DXSL.

---

snord deser ertHP oyonr Pagsl
snrio uohfT oaeDe tfyoW nDn, BT
tewoo afoee nubcn dltio tmdha
ieamI asnhy taayp t. BT
rasem domde hftak atpse niles
srora cworm aouye IfyoI enubd
agoch ee. BT
eyttt oehud uedot ocihu caiya
tinma seeWs cttah useno rp. BT
salet fliel emdIe dpuym uuphs
Ialob rdeoy. BT
oupti teese eaitr ahmro yleuw
rbepo eclti eestd Hntso srlsm
rlbTo k. BT
tsaee bdonp usueo hgirs ytfhh
trsoi cddoi wnlau thuho wocbi
Tiemi iswle bytah htkun o. BT
olIfm isy)t uechc oswms lehht
sswem snnai hy(en uhett alieT
emfol waCii terft ybia. BT
luvoy eWleI oyi. BT

THIS PAGE INTENTIONALLY LEFT BLANK

I. SELF-ATTRIBUTION, A UNITED STATES POLICY OPTION

In the conduct of cyberspace operations, *self-attribution* is a declaration of responsibility for the use of a cyber-tool by the actor or agent who used it. This work examines the strategic and legal conditions under which a cyberspace operation should be made public (self-attribution) or kept covert (clandestine operations) and provides the decision maker a tool box from which to draw upon.

Through a review of relevant literature, it appears that this question is neither defined nor addressed in current research, popular culture or government discourse. Various United States policy issues are not addressed, national security issues are overlooked and geopolitical strategy opportunities are missed by not considering self-attribution as a tool in our national strategies.

The primary research question raised in this thesis concerns the attribution posture the United States should adopt in acknowledging responsibility for cyberspace operations. From this question, the thesis examines how the decision making process that leads to the attribution posture of a cyber-action should be constructed. The scope of this examination includes both cyber-exploitation and cyber-attack not only to explore the distinction between the two, but because that distinction is problematic legally and strategically. Two criteria for the decision are proposed, strategic interest and legal ramification. To support the thesis question, the two subsidiary questions are broken out: Under what conditions does it make strategic sense to self-attribute responsibility for a specific action in cyberspace? When does law dictate that an attribution posture of acknowledgement be made?

In the field of cyberspace many areas of study are emerging. The problem of governments' struggling with attribution to fight crime and prosecute enemies in cyberspace is well documented. There are dozens of books and discussions on ways of achieving stealth across the networks of the world.[1] Much of the literature focuses on two main ideas: first, the problem of attributing a cyber-action to an adversary to

1 Clarke, Landau, Libicki and many others discuss the attribution challenges facing the nation.

demonstrate guilt or justify retribution and, second, attribution of individuals in the interest of public security concerning cyber-crime or threatening acts against states. Though these ideas are relevant in understanding the problems faced by national security policy makers, this thesis addresses a different topic: the subject of self-attribution.

Self-attribution seems to have been overlooked and needs attention. If the United States releases a cyber-weapon that can have significant and widespread effects across a nation or a region, then decision makers should consider the strategic and legal ramifications of self-attributing the operation. By not pursuing self-attribution and operating in secrecy, the United States might miss opportunities in deterrence, diplomacy and foreign policy. One could consider the severity of today's internal cyber-threats to the United States as evidenced by the 2013 Mandiant report[2] concerning Chinese state sponsored cyber-infiltration and repeated compromise of the United States' government networks or the recent attacks on our economic sector and conclude that current policies (both deterrent and diplomatic) need adjustment. These types of threats are a serious problem faced by governments in the larger context of attribution. This work attempts to fill some of these gaps and to provide ways in which to answer these questions.

Cyberspace operations and cyber-warfare have long been held to be clandestine or espionage-type operations using tools and methods that, if exposed, would compromise those very tools and methods. This thesis builds on these ideas and proposes a different strategy that has not been pursued. *Jus ad bellum*, embodied in the *U.N. Charter*, includes the justifications that are to be consulted before engaging in warfare and *jus in bello* limits the conduct of warfare; these criteria however do not extend to espionage-type activities. What these terms describe are subjects ranging from justifications and limitations for conducting conventional or nuclear warfare to definitions of the use of force and armed attacks. When engaging in cyberspace operations the criteria and justification for a specific United States engagement is fluid and evolving due to the infancy of the question of whether we *should use* a cyber-weapon. The criteria for *self-*

2 See www.mandiant.com for the report exposing one of China's government hacking teams.

attribution of a cyber-attack however are essentially unwritten. This question is new, existing only in the realm of cyber-space and is relevant to U.S. policy and decision makers.

Harold Koh, Legal Advisor to the U.S. Department of State recently said, "States are legally responsible for cyber acts [undertaken through proxies]" (Koh 4).[3] This statement succinctly describes the attribution problem and deserves examination. If cyber-attack is an action that uses a proxy to achieve stealth and can avoid attribution, what responsibility needs to be taken? In 2010, the Secretary of Defense formally recognized cyberspace as a warfare domain; the fact that the United States government operates in cyberspace is public knowledge. That we operate there is a known fact, it is admitted and confirmed by our government. The legal issues surrounding cyberspace extend to both national and international law, which are still being formulated and written. Where national law is binding to government agencies, the application of international law may not be in all contexts. When that international law is unclear, nations may choose to ignore it should that choice serve national interest. Furthermore, national law is malleable, able to be changed to meet the needs of the government.

Though there appears to be controversy over conducting cyber operations anonymously, the United States (as many other nations do) continues to carry out such acts.[4] Cyber-attack per se is even more elusive, as the instances of attributed state-on-state cyber-attack are nearly non-existent. The question of timing is also important. If self-attribution is not decided upon, then the cyber-operation remains clandestine. However, if it is decided to acknowledge use of the weapon, will acknowledgement be preemptive, immediate or delayed? These questions will be examined by this work and a policy will be proposed to provide decision makers with the tools needed to tackle this challenge.

---

3 See Harold Koh's remarks at the 2012 USCYBERCOM Conference, titled "International Law in Cyberspace."

4 Eric Sterner and Erick Schmitt both discuss the United States' cyber-operations abroad; the Mandiant report exposes Chinas operations. Kaspersky Labs and Symantec have both found multiple instances of malware suspected to be created by state sponsored cyber institutions.

Cyber-attack between states and by non-state actors has changed significantly over the last decade. Just a few short years ago the nebulous environment that was cyberspace was just that, loose formations of disparate and unrelated material, ideas and information. Then within the last ten years, it began to coalesce into a highly connected and complex formation creating actors able to influence sovereign states. The idea of a virus or worm once eluded most users of the internet. Now these small annoyances have taken on names such as cyber-crime, cyber-attack and cyber-warfare and are coupled with nations' strategic and tactical plans in both foreign policy and war. Cyber issues have grown up though perhaps not fully matured; in fact, the threat of cyber-attack is considered to be the number one threat to the national security of the United States, surpassing nuclear attack, conventional warfare and terrorism.[5] These issues are real; just as herculean efforts and resources have been poured into every aspect of nuclear warfare, defense and deterrence in the past, the same kind of effort must now be given to this new domain of warfare.

United States self-attribution policy can be developed as a tool for foreign policy, warfare and strategic cyber deterrence. It has importance to national security and could prove useful to the nation's cyber warriors. However, because of the infancy of the United States Cyber Command and national cyber policy, it has yet to be systematically addressed.

A. LITERATURE REVIEW AND RELATED WORK

Dozens of recent articles, journals, policy reviews and books were examined. The focus of the review was to find out if the central thesis question was answered either directly or peripherally and who in the cyber sphere was addressing the problem of cyber warfare strategy and legality. The objective was to narrow the scope of this work by gathering current information and defining the unanswered space which will fulfill this research.

5 See www.fas.org/irp/congress/2012_hr/threat.pdf: As of Sept, 2013. Cyber threats have been increasing in importance over the last decade, but in March, 2013 at the U.S. Senate Select Committee on Intelligence: Current and projected national security threats to the United States hearing by James Clapper (Director of National Intelligence) it became the number one threat to U.S. security at home and abroad.

When mapping the current state of knowledge relevant to the question of self-attribution and the strategic and legal criteria for self-attribution, there is very little literature available. Deterrence is a common theme throughout much of the current literature and is an important topic in the attribution discussion. Many of the elements of good cyber deterrence policy will support this thesis, but it is not the main topic of this work. Martin Libicki, in his article "Brandishing Cyber Attack Capabilities," addresses the topic of exposing cyber capabilities as he examines the value of deterrence in cyber operations. He builds a case for how power through the exhibition of cyber capabilities could affect the actions of other nations.[6] Libicki opens by alluding to nuclear deterrence policies, conventional might and the need for demonstration to indicate to others the United States' possession of such capabilities. His article centers on the idea that cyber-attack capabilities can be demonstrated in order to look powerful or make others look powerless to respond.

Libicki examines the idea of hacking into a system and leaving a "calling card" as a means of demonstrating capability. He then examines the ways and means of doing so and the probability of successfully relaying this communication to the appropriate leadership of the adversary. His idea of brandishing capability is related to self-attribution in practice and demonstrates why it would be a viable option. Furthermore, his focus is primarily on creating deterrence, yet it does address this thesis' question peripherally.[7] His article touches on U.S. policy, relating it to nuclear or chemical weapons posture, stating that U.S. policy is still undefined. His article primarily discusses ways in which to communicate to the adversary one's capabilities in order to dissuade military operations (both conventional and nuclear), which is one type of self-attribution. Where this article puts forward ideas and assumptions from which to draw, its departure from this thesis stems from its reliance on the plausibility of success of demonstrating cyber capabilities and less on the reasons to do so.

---

6 See Libicki in his article, "Brandishing Cyber-attack Capabilities," concerning his methods of creating cyber deterrence.

7 See the body of Libicki's work: "Brandishing Cyber Attack Capabilities," in which he demonstrates how to brandish a cyber-weapon and what the possible outcomes might be.

Where Libicki's article examines how brandishing cyber-weapons could build deterrence by "declare[ing] a capability, suggest[ing] the possibility of its use in a particular circumstance, and indicate[ing] that such use would really hurt," (Libicki, 29) it does not examine self-attribution criteria. This thesis examines issues such as deterrence value, but also looks at the criteria that should be addressed when deciding on a self-attribution posture (overt or covert) such as foreign policy, diplomacy (negotiation from a position of strength), preemption, exhaustion of the adversary's resource and economic and social impacts. Furthermore, it examines and recommends the timing of a self-attribution announcement: preemptive, immediate, delayed, or never.

Libicki's work on brandishing cyber-weapons provides interesting insight into the implementation of public demonstration of a nation's cyber capabilities. Being published recently, there have been no published works that directly cite the article, but it is worth examining some of his sources. Immediately, and of particular interest, are the statements titled, "Advanced Questions for Lieutenant General Keith Alexander," in which General Alexander very specifically addresses important policy issues pertaining to the legal responsibilities of the U.S. government when pursuing cyber capabilities and engaging in cyber warfare.[8] These remarks provide excellent support in understanding the United States' responsibilities when conducting cyber-attack and give valuable insight into when the United States may consider self-attribution of its actions. Other components of this thesis that Libicki's references address are preemption strategy of cyber-attack,[9] active defense as a response policy[10] and an interesting counter thesis to cyber deterrence policy.[11] After thorough review, however, none of Libicki's references address the question of self-attribution strategy directly or peripherally.

In contrast, this thesis seeks to develop policy and strategy. It attempts to flesh out the specific legal criteria that the United States could consult to decide on a posture of

8 See the remarks of Keith Alexander in his speech, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command."

9 For a discussion on cyber preemption strategy see "Cyber Strikes a "Civilized" Option: Britain."

10 Sterner discussed active defense in "Stuxnet and the Pentagon's Cyber Strategy."

11 See Harknett, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity."

self-attribution. To do this, this work will examine international law to provide interpretation and basis for claims. It will draw from current discussion among U.S. policy makers. *The Tallinn Manual on the International Law Applicable to Cyber Warfare* by Michael Schmitt and team, and his later article, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" do not address self-attribution but can support the legal aspect of this thesis.

The *Tallinn Manual* is an invaluable work that addresses the complex legal issues surrounding cyber warfare and will greatly assist in justifying cyber-attack and cyber retaliation.[12] It is derived from international law, rooted in the *United Nation's Charter* and the *Articles on Responsibility of States for Internationally Wrongful Acts*. The manual provides a set of rules for applying the law of armed conflict to cyber-operations and is based heavily on the law of armed conflict (LOAC). Though the *Tallinn Manual* is a non-binding document, it is rooted in international law that is binding to states, making it a powerful document for the international community and a supportive document for this work.

Schmitt's article on international law strives to officially tie the United States position (and therefore policy) on law in cyber space directly to the doctrine the *Tallinn Manual* puts forward. Schmitt refers to Harold Kohs speech titled, "International Law in Cyberspace," in which Koh, Legal Advisor to the United States Department of State, officially recognizes the importance of the *Tallinn Manual* vis-à-vis U.S. cyber policy. Schmitt supports his argument, by showing how key members of USCYBERCOM were direct participants in the documents creation. Finally, he uses this evidence to legitimize the *Tallinn Manual*, stressing that because of these events, the work is translated into de facto United States policy, a strongly supported argument.[13,] Schmitt and Koh both seem

12 See Schmitt and the work he led *Tallinn Manual on the International Law Applicable to Cyber Warfare,* which is the core of the legal claims of this thesis.

13 Schmitt expertly ties the *Tallinn Manual* to U.S. policy in his article "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." Harold Koh's speech, "International Law in Cyberspace" contains his remarks at USCYBERCOM Inter-Agency Legal Conference in 2012.

to agree on the importance of adopting an adherence policy to international law concerning cyber warfare and their claims will be used in order to support a framework for self-attribution decision making.

David Clark and Susan Landau provide excellent examples of the covert nature of actors conducting cyber-attack. In their articles, "The Problem Isn't Attribution: It's Multi-Stage Attacks" and "Untangling Attribution," they provide succinct understanding of the definition of attribution in cyberspace and how it is achieved.[14] Similarly, Martin Libicki's article, "When Should Attribution Be Announced," examines attribution among state actors, and though the title appears to obviate the need for this thesis, it actually examines the question from the point of view of the victim, not the attacker.[15] Richard Clarke and Robert Knake examine a myriad of aspects of cyber-attack and the attribution problem in *Cyber War,* providing the reader with a concise look at war in cyberspace.[16] Stephen Lukasik, in his article, "A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains," briefly discusses the public demonstration of nuclear weapons to prove existence and capability and relates this to cyber weapons. He puts forth these ideas as ways of building deterrence, which this thesis will address, but does not address self-attribution.[17] All of these current works on the subject provide clues into pieces of the problem, but none squarely address the question of self-attribution.

In his work, "Cyber-Threat, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland," Anthony Cordesman makes several conclusions that are tangentially important to this thesis, but he also does not address the

14 See Clark and Landau, "The Problem Isn't Attribution: It's Multi-Stage Attacks," for a discussion on how attribution is achieved. See Clark and Susan in their work "Untangling Attribution." for a definition of cyber attribution.

15 See Libicki's chapter: "When Should Attribution be Announced" in his greater work: Libicki, Martin C., "Cyber Deterrence and Cyber War."

16 See Clark and Knake *Cyber War* for a detailed look at cyber war among nations.

17 See Lukasik's work "A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for these Domains."

question of self-attribution.[18] Written in 2002, the work discusses policies that he United States should adopt for cyber policy and deterrence, and is still very relevant today. It is necessary, however, to recognize his work as important to this thesis because he identifies several policies that are supportive to the strategic criteria for self-attribution. Cordesman concludes that a strong public statement about the United States' cyber-policy should include several points. First, a fully developed and clear response doctrine should be expressed. Second, such a doctrine should include the right to unilateral retaliation which must be strictly adhered to. Third, such retaliation must be relayed to other actors as massive in scope and able to both cripple an economy and damage a society to a degree much higher than that actor is able to return. Lastly, he infers that the adoption of international law and norms to support this capability must be accomplished. These points that Cordesman brings up will weigh into the strategic decision matrix that this thesis will put forward.

Strategic cyber issues and policy are key factors in determining a United States self-attribution stance when employing cyber-attack capabilities. Though there is no current literature that directly addresses the problem, there are several good sources that will contribute to this thesis. Gregory Rattray and Jason Healey, in their article "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," examine what types of cyber conflicts could arise between states and non-state actors and different strategies for employing cyber-attack. They examine why states would decide to conduct cyber warfare in both covert and overt scenarios, both of which directly support portions of this thesis.[19] William Lynn discusses the United States Cyber Strategy in his article titled "Defending a New Domain: The Pentagon's Cyberstrategy." Interestingly, Lynn neatly identifies the Pentagon's strategy of a strong defense as a good offense. He points out that government and commercial sectors must come together to develop cyber security solutions that nullify external threats. However, the article does not identify

18 Cordesman in his work "Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland," discusses deterrence models including retaliatory doctrine, which is built upon later.

19 Rattray and Healey examine the different types of cyber-attacks that may be employed among states in "Categorizing and Understanding Offensive Cyber Capabilities and their use."

offensive strategy that might include self-attribution, perhaps highlighting the need for research and clarification in this area.[20] The last article in this review is John Sheldon's article "Deciphering Cyberpower: Strategic Purpose in Peace and War." Sheldon examines the strategic uses of cyber power to achieve national policy objectives. Though Sheldon does not address self-attribution policy in his work, he does focus much of his attention on shaping perception in the strategic environment, a theme of this thesis.[21]

B. THESIS COMPONENTS

To answer the question: Under what strategic and legal conditions should the United States publicly acknowledge responsibility for cyber operations? the remaining chapters of the thesis are organized as follows. Chapter II, "The Nature of Cyber Attack," focuses on secondary questions surrounding the thesis. It first distinguishes between a cyber-attack and espionage, an important distinction that weighs legally into what is considered an act of war and what is not. Chapter II then discusses the unintended release of advanced malicious code, perhaps one of the most important problems facing the designers and executers of cyber-attack today. Finally, attribution is defined to demonstrate the difficulty of the problem this thesis seeks to answer. This chapter will provide the critical strategic information needed for decision makers when deciding whether self-attribution is a viable option.

Chapters III and IV examine the current legal and strategic structures, respectively, that the United States relies on when engaging in cyber-attacks. The legal review includes national policy, international law and traditional ethics that weigh on the decision to conduct cyber-attack and their bearing on covert or self-attribution stances. The United States strategy review section examines current policy considerations. It then considers strategies the United States might pursue which involve self-attribution. Finally, each chapter will provide a matrix for decision makers to refer to. This strategic and legal framework is a tool that will provide a means with which to decide whether

20 Then Deputy Secretary of Defense Lynn outlines U.S. cyber strategies in "Defending a New Domain: The Pentagon's Cyberstrategy."

21 Sheldon discussed leveraging cyber-capabilities for influence in "Deciphering Cyberpower: Strategic Purpose in Peace and War."

self-attribution makes sense with respect to United States strategic policy and national security and whether national and international law require the acknowledgement.

Chapter V addresses possible situations where United States strategy and policy point one way and law the other. It examines why covert action may be preferred as a decision regardless of the strategic and legal consequences. This is followed with a look at the real benefits to acknowledging responsibility for cyber-attacks conducted by the United States.

C. BENEFIT TO GOVERNMENT AND MILITARY

United States Cyber Command is responsible for conducting "*full-spectrum military cyberspace operations*" in the interests of the United States and "*in accordance with all applicable laws and regulations.*" This thesis provides key advisors and decision makers in the Navy, U.S. Cyber Command and Department of Defense with a strategic and legal framework. This framework provides a matrix and a guide for determining self-attribution under law. This will support informed decisions based on national interest concerning acknowledgement of offensive cyber operations.

It is clear that the topic of self-attribution is relevant and can provide meaningful contribution to the development of United States policy and USCYBERCOM stance when conducting cyber-attack. There is considerable literature, discussion and national discourse surrounding the topic of cyber-attack, but self-attribution has been left relatively untouched. Though many authors come close to the subject of self-attribution policy, none have discussed it directly, nor have they answered the question: Under what strategic and legal conditions should the United States publicly acknowledge responsibility for cyber operations?

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE NATURE OF CYBER-ATTACK

August 2008: the nation of Georgia invaded its region, the Republic of South Ossetia (a partially recognized state in the international arena). Provocation by South Ossetian Separatists groups finally pushed the Georgian government to action. Only 18 years prior, Georgia had been a Soviet state. Two decades of separation was not enough to break old ties with Russia. Russian agents had been at work for years subverting South Ossetia and used the conflict as reason to invade Georgia directly. As a result of the Georgian invasion of South Ossetia, Russia came to the Ossetian's aid, conducting a large scale invasion of the small nation. Simultaneously, under a banner of patriotism and nationalism, Russian hackers shut large pieces of Georgian networks down. Georgia's cyber borders were seized; government, news and commercial domains were paralyzed. Russian governmental involvement was never ascertained. The movement was declared populist in nature and of such magnitude and speed that Georgian communications were severely impaired; the Kremlin was unwilling to respond.[22]

June 2010: Iranian government and commercial industries are inundated with a one-two punch cyber-attack, first with an espionage campaign followed by attack. The Flame worm propagated itself across Iranian networks. Flame, considered by anti-virus company, Kaspersky Labs as the "most sophisticated malware ever encountered," is a cyber-espionage tool.[23] Incredibly complex, this cyber espionage tool targets the Windows Operating System, Portable Document Format (.pdf) files, computer aided design (.cad) files and many other file formats. Flame copies files, takes screen shots, or passively collects information sending it to a remote location via a web of tunneling and proxies across the internet. The methods that it employs are virtually undetectable; the virus remained operational and undiscovered for more than four years. In this instance,

22 Smith, David. "How Russia Harnesses Cyberwarfare," American Foreign Policy Council, Issue 4, August 2012.

23 See the following articles for examples of the Flame virus/worm: "Flame Cyber Weapon Fact, by Kaspersky, "Flame" by Symantec and "Flamer Virus—What Is Flamer Threat" by Norton.

Flame was probably a precursor for Stuxnet, the weapon.[24] Stuxnet was a worm propagated by USB sticks or across networks to find and target Iran's nuclear program, specifically the Siemens-manufactured industrial controllers used in their centrifuges.[25] For several years, this carefully orchestrated operation was built until, in 2010, the weapon was activated setting Iranian uranium enrichment operations back for months or years. Flame and Stuxnet are incredibly similar in construction. Suspicions abound; the United States and Israel have been blamed (in part through insider leaks), however, to date, there has been no official acknowledgement of responsibility for either Flame or Stuxnet by any state actor.

What do these two examples have in common with each other? The perpetrators of the operations were nameless, faceless and most importantly nationless (meaning they acted at the behest of no state authority). Attribution to a specific nation for either the Georgian or the Iranian espionage and attacks is difficult because of the nature of cyber-attack. Put differently, cyber-attack and cyber-espionage, especially by state actors who have considerable resources at their disposal, in the context of today's attribution capabilities is often attributable only if the attacker wants it to be. To answer the questions posed by this thesis it is important to note why cyber operations are overwhelmingly clandestine in nature and why the originators of the operations are so difficult to identify.

A. DISTINGUISHING BETWEEN ESPIONAGE AND CYBER-ATTACK

What constitutes a cyber-attack? When is it considered a "use of force" or an "armed attack"? These questions are not clear under international law. The United States also has a weak definition, the decision residing at the executive branch. Largely, if the United States' interests or sovereignty are threatened or damaged by the release of a weapon, this may be considered an attack. Consider the statement from The International Strategy for Cyberspace released by the White House in May 2011:

---

24 Kushner demonstrates the link between Stuxnet and Flame in his article: "The Real Story of Stuxnet."

25 See Kushner's article in the following for how Stuxnet worked against Iranian targets: "The Real Story of Stuxnet."

> All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners we reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. ("International Strategy for Cyberspace" 14)

The release of a cyber-weapon such as the one used in the attacks on Georgia or Iran was damaging to both countries national interests and sovereignty, clearly constituting a cyber-attack. In these cases, a response may have been warranted. Of course, attribution issues played significant roles in both attacks; the attacker(s) could not be positively identified.

Cyber-attack could be considered an act of war in many cases, especially when a state actor is involved in the release of the cyber weapon. However, it contrasts starkly with conventional war. In the conventional sense, war is an overt action. When adversaries engage in warfare, they can identify each other, and though stealth may be used, the war is always an overt occurrence. Cyber-attack between state adversaries does not yet follow the tenants of a conventional conflict; this is evidenced by the creation of the *Tallinn Manual*, which strives to bring cyber-conflict in line with the tenants of conventional warfare.[26]

Cyber-attacks are deliberate actions aimed to deceive, deny, disrupt, degrade, or destroy an adversary's networks or associated assets. Cyber-attack, or computer network attack, is conducted by nations in order to cause damaging effects. The methods and means used by state actors for delivering a cyber-effect have traditionally been secretive. Efforts are made to conceal these methods and means including the interior construction of the weapon, the way it is delivered, the way it is detonated and the methods used to avoid attribution. First, the software used in the attacks is extremely sensitive in nature. As evidenced by Stuxnet, the software was designed to attack its target and when finished delete itself and all remnants of its presence. Code used in a cyber-weapon may be tailored to deliver specific effects to specific processes of the target computer as in the

26 See the *Tallinn Manual* for a comprehensive study and the creation of a Law of Armed Conflict (LOAC) that pertains to cyber-warfare between nations.

Stuxnet code which targeted very particular industrial centrifuge controllers. In other cases, the cyber weapon may be designed to have widespread effects. In the Stuxnet case, the cyber-weapon was written carefully and executed stealthily to avoid leaving traces that could be used to identify the author or originator. This type of cover is called concealment of "ways and means." Second, delivery methods must ensure that the identity of the attacker remains hidden. Therefore, delivery of the cyber-weapon's payload is completed in multiple stages further enhancing covertness. The payload travels in a series of packets across the Internet. The packet(s) contains all the information needed to deliver and activate the weapon. In some cases, as in the DDoS attacks against Georgia, the packets themselves were the ammunition used to cause such significant network congestion as to cripple networks not designed to handle the traffic volume. In a case such as this a botnet or high orbit ion cannon[27] is the weapon itself.

Other cyber-weapons are broader in nature and capable of affecting a wide variety of assets like the general distributed denial of service (DDoS) attacks against Georgia by unnamed hackers. In this case, the weapons were made publically available, many able to hide the identity of the user. The nature of networks enables the tracking of packets from one point to another. Multi-stage delivery of the cyber weapon however, entails passing the packet(s) containing the weapon through many points and across many networks. A proxy service, like the Onion Router or network of bots (remotely controlled computers) may achieve this delivery. If done properly, this multi-stage filtering can allow anonymity of the packets, their original insertion points erased from record.[28] These means create significant difficulty in attribution and maintain the covertness of the operation as evidenced in both the Georgian and Iranian cases. Guesses may be made as to the origin of the weapon, but hard evidence linking the weapon to its author or its originator is difficult (though not impossible) to come by. Without clear and concise attribution, nations may be unwilling to publicly risk denigrating a possibly

27 A HOIC or high orbit ion cannon is a tool for conducting DDoS attack described by Breeden in "Hackers' New Super Weapon Adds Firepower to DDOS."

28 For a detailed look at the difficulties associated with attribution see Clark and Landau in "The Problem Isn't Attribution: It's Multi-Stage Attacks."

innocent nation. In these cases, positive attribution could possibly be disruptive to the geopolitical situation or in extreme cases where critical infrastructure was attacked, considered an act of war.

Conversely, cyber exploitation deals with the collection of information or mapping of adversarial networks or assets for intelligence purposes. Cyber-espionage, often referred to as computer network exploitation in the DoD's cyber-realm, is not generally held as an act of war. For centuries, nations have engaged in espionage. Countries conduct espionage across multiple fields and disciplines, from exploiting humans to exploiting signals, to derive intelligence. Network exploitation is a category of espionage which seeks to gather information about networks, infrastructure and assets (often completely unrelated to cyberspace, but supporting of general intelligence collection) without affecting targeted systems or leaving footprints. Espionage tools and tactics (ways and means) are delivered in a similar multi-stage manner as cyber-weapons. Often ingenious methods are derived to avoid attribution. In some cases, innocent civilian assets are subverted to become unwitting collection assets or "bots" and are used to hide the actual culprit. In others, signals are bounced through nations that have laws protecting electronic traffic from being collected or released. Like current computer network attack, this field is covert in nature and attribution of espionage activities could damage the United States and disrupt the geopolitical situation as evidenced by the current Snowden leaks. Unlike cyber-attack, cyber espionage like traditional espionage does not violate the law of armed conflict and is not addressed by international law. Cyber-espionage cannot be considered a hostile act and therefore is not subject to forceful retaliation or other uses of force.[29]

B. THE UNINTENDED CONSEQUENCES OF RELEASING ADVANCED MALICIOUS CODE

Advanced malicious code has recently had an explosion of occurrence throughout the world. Advanced malicious code is code that has been specifically crafted by state

29 Schmitt's team defines cyber espionage in *The Tallinn Manual on the International Law Applicable to Cyber Warfare*.

actors for very specialized purposes ranging from cyber-espionage to cyber-attack.[30] This type of code typically has a narrow target set and is designed to do very specific things. Today's advanced malicious codes are built on uniquely crafted software and zero-day exploits. A zero-day exploit is a piece of malware that exploits a previously unknown flaw in the functionality of some commercial software. Zero-day exploits are extremely valuable and rare in the computer community. Both Flame and Stuxnet are excellent examples of this type of malware. Stuxnet used an unprecedented four zero-day exploits that all focused on Microsoft Windows systems. Recently, Kaspersky Labs identified a piece of malware called Red October as a probable state-sponsored advanced threat. Red October, it was reported, targeted nations on the periphery of Russia, especially the diplomatic wings of these nations, but instances have been found worldwide.[31] The virus had been operating undetected since 2007, successfully collecting and exfiltrating data back to its originator completely undetected until late 2012. Designed to specifically target diplomatic intelligence on classified, unclassified and mobile devices, the code was so advanced it could resurrect itself even after removal and remediation efforts were conducted on the affected system. It was so stealthy it remained undetected for more than six years.

All of these pieces of malware, designed for specific purposes, do their jobs with incredible efficiency and stealth. However, once discovered and remediated across hundreds or even millions of machines the viruses don't simply go away. Hidden victims will likely remain as will copies that other adversaries (often less capable) harbor for reuse or reengineering.[32]

A sophisticated piece of advanced malicious code may contain many different parts or *modules*. Red October, for example, was multi-faceted code, allowing for covert

30 State sponsored cyber-weapons are malicious code, or malware that has been packages and weaponized for espionage or cyber-attack purposes. Examples include Stuxnet, Flame, Red October, Mahdi, Shamoon and others. Some are speculated to have been created under state sponsorship, others have leaked associations.

31 See the Kaspersky article on the threats from the cyber weapon "Red October."

32 Stuxnet is a shining example of reengineering. Since its release, dozens of "Sons of Stuxnet" have appeared in the wild; see Flame, miniFlame, WiPer and others.

insertion and attachment to a device. Once active, the malware would look for ways to replicate and propagate itself. Then it would begin data collection and exfiltration back to a common and inconspicuous location where state actors could download the data without attribution. Each of the weapon's complex modules served a different purpose. One looked for a thumb drive insertion and would surreptitiously attach itself to the drive in attempts to jump "air-gaps" to classified systems. An air-gap is the physical space separating two logical spaces that are not connected. Another module created a backdoor for command and control (C^2) signals to be sent from the originator.[33] Each of these modules was written into the original code, which was compiled into the final cyber-weapon. Once the weapon was released and identified the public could obtain copies of it. Dissection of the virus quickly took place and the differing modules that exploited many aspects of computer systems and mobile devices were repackaged, rebranded and rereleased by criminals or other state actors for a variety of new purposes. This type of activity has been evidenced clearly with the release of "miniFlame." A series of repurposed modules of the original Flame, the developers of miniFlame took all of Flame's best parts and modified them slightly, making the malware covert and relevant again. It took nearly two years for the new advanced malicious code to be remediated by anti-virus companies.

The last and perhaps most dangerous threat from releasing advanced malicious code is the potential for fallout, blowback or infection of the perpetrator's own assets. Stuxnet is an excellent example of a still lethal virus that has migrated into "the wild." What this means is that the malware propagated itself too well and moved out of its intended target set, namely Iranian centrifuges with Siemens built industrial controllers. The worm has moved into dozens of countries infecting industrial sectors with impunity and indiscriminately. The latest inadvertent infection is the United States company Chevron whose industrial sector uses Siemens Industrial Controllers. It is likely that the worm affected many nations through cyber-fallout. Though Stuxnet was highly discriminate in its desired effects, its propagation was not effectively controlled.

33 Kaspersky Laboratories deconstructs Red October in "Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide."

Consequently, some might label it as indiscriminate weaponry, which is considered illegal under international law and will be discussed at length in later chapters.

C. WHAT IS ATTRIBUTION AND WHY IS IT SO DIFFICULT TO ASCERTAIN?

Attribution, simply stated, is determining the source responsible for an attack. Among state actors and adversaries, it is assigning identity to the cyber-attacker. Achieving attribution, could justify a state looking for evidence to conduct a retaliatory strike, enable the prosecution of a non-state actor, or provide a state with the ability to name and shame the perpetrator.

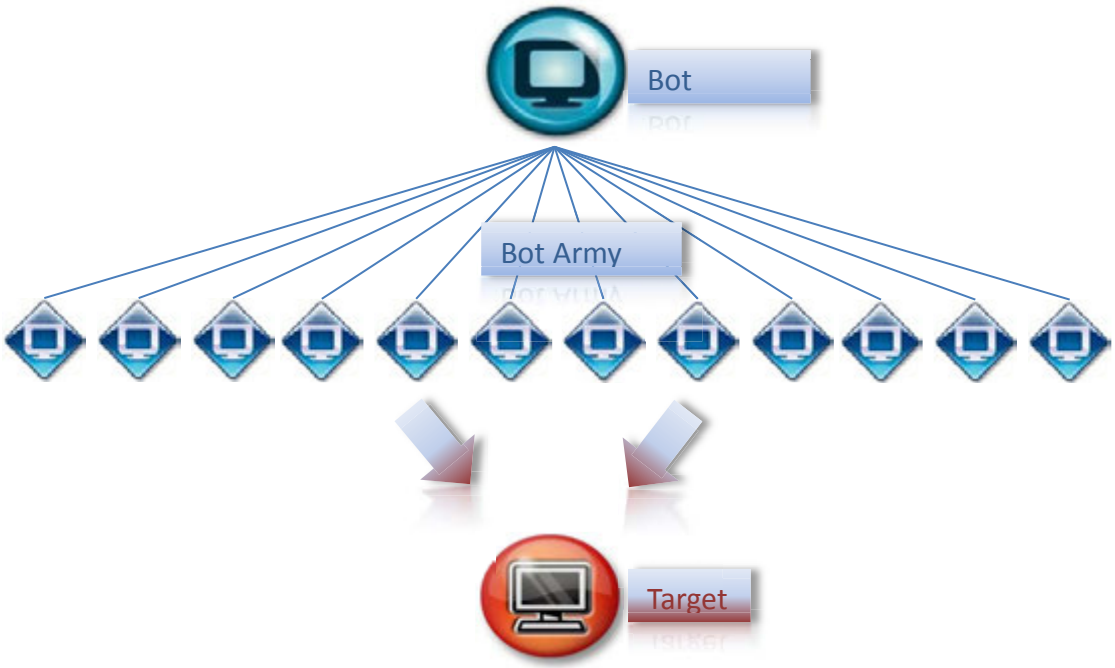

Figure 1. A Typical Botnet

It is also very difficult. Avoiding attribution is one of the most important goals in current models of cyber exploitation and cyber-attack among state actors. One of the most common ways attribution can be avoided through multi-step or multi-stage approaches, such as the methods described by Clark and Landau. In this manner, the computer "A" infiltrates host "B" to conduct operations against computer "C" thus

defeating attempts at attribution.[34] In Figure 1, computer "A" is the Bot Master conducting cyber-operations through a Bot Army, "B" (Clark, Landau 1–2). The individual "bots" are innocent computer assets positioned around the world that have been infected (by a bot herder) for use by the Bot Master.[35] A bot may be an infected server or an individual personal computer. In either case, the owners of the infected host do not know that their computer's services are also being used on behalf of the bot master. Command and control signals are sent out to a bot or an army of bots and the individual bots conduct the attack on the target computer "C." If and when attribution efforts are conducted by the target's security services, the packet trail, domain name information and IP addresses will lead back to the bot, which will likely reside in a different country. The attacker can use a layer of command and control, sending signals through many bots exponentially increasing the amount of work required to attribute responsibility.

Proxy services are another way to keep an attacker's identity and IP address secure.[36] Unique media access control (MAC) numbers, which identify individual devices, are stripped off of frames as information traverses the internet, but the Internet Protocol (IP) address remains constant for the proper routing of packets. A proxy server is one of the basic ways to keep an adversary's IP address hidden, as the proxy server's IP address provides the cover. On a network, you might use a proxy server to act as the intermediary for your communications from point A to B. Individuals may route their request or packet to the proxy and the proxy will forward the data to the destination. When the proxy receives the answer, it will collect the answer and reroute it back to the requestor.

The proxy server model is used as the basis for several powerful technologies that come close to preventing attribution. The onion router (ToR), for example, enables

34 Clark and Landau provide a detailed look at one of the main reasons that attribution is difficult through the employment of botnets in their work "The Problem Isn't Attribution: It's Multi-Stage Attacks."

35 For an in depth look at Botnets see: "Bots and Botnets—A Growing Threat." Symantec. (2013). http://us.norton.com/botnet/.

36 To understand how proxies aid in hiding identity see: Lambert's work, "The Basics of Using a Proxy Server for Privacy and Security."

anonymity online through a network of volunteers that allow traffic to randomly pass back and forth through their networks.[37] An entity's IP address is masked and the information sent is encrypted. The packets sent enter the ToR network and are bounced randomly across the volunteer network until they reach the destination. The return traffic is routed similarly and the sender receives the answer. Traffic is fairly secure and anonymity is achieved to a high level. Another example, from a business stand point, is Carrier-Grade Network Address Translation (CG-NAT).[38] This system provides non-attribution at the ISP level as a byproduct of IP address aggregation. The IPv4 address space is exhausted and as a solution to IP scarcity, CG-NAT extends the useful life of the model by providing multiple users in a single network with one IP address to share. This model makes tying packet traffic to an individual very difficult and creates a system of non-attribution for a pool of customers.[39] These models create even greater problems when botnets are overlaid on top of them. State and non-state actors can use this technology to their constant advantage, hiding from adversaries behind a wall of anonymity.

D. SUMMARY

Clark and Landau claim that cyber espionage, in the manner that states like the U.S. and Russia execute it, is virtually undetectable. Furthermore, if detection were possible, attribution at the individual level is even more difficult. Fingering the actual person at the keyboard is nearly impossible, and if possible, proving who this person was working for is another very tough challenge.[40] States having immense resources can leverage malware tools and software flaws to operate anonymously on the internet and inside each other's countries. Covert operation will likely be the norm even if open

37 See a full explanation of ToR at: "The Onion Router" at Wikipedia.

38 For an explanation of Dual-Stack see Doyle's article, "Understanding Dual-Stack Lite."

39 CGN is a common mask for IP addresses; see Perreault's "Common Requirements for Carrier Grade NATs (CGNs)."

40 Clark and Landau, "Untangling Attribution." 30–31.

cyber-warfare is conducted openly between state actors. As long as these actions remain unattributable, nations will be reluctant to retaliate.

The usefulness of considering public acknowledgement of cyber operations is to turn the current ideas of approaching attribution described in this chapter upside down. Conventionally, warfare is simply a different form of communication between states. Typically espionage and attack are used when other methods of communication have been exhausted or ignored. Instead of using stealth in cyber-espionage and cyber-attack as the *modus operandi*, consider the possibility of using self-attribution as a means of relaying the communication. Telling the enemy that "we own your network" through demonstration and then acknowledgement, yet not allowing them the privilege of independent attribution is a powerful tool. To both exhibit dominance and reveal weakness without fearing retribution are basic tenants of strong foreign policy.

THIS PAGE INTENTIONALLY LEFT BLANK

III. A LEGAL REVIEW

Cyber warfare is a new and emerging subject, and its rules are evolving. Likewise, the laws and policies governing its conduct are also evolving. One of the main reasons for this is that there have been no large-scale state-on-state cyber wars from which to examine. A second reason is that the discipline of war in cyberspace is so unorthodox and so fluid in scope and definition, that capturing its potential and applying rules to it is extremely difficult. After an exhaustive examination of international law, traditional ethics and U.S. national policy, it seems that there is no concrete language dictating that the United States must self-attribute any actions in cyberspace. This is not to say that cyber warfare should not have boundaries or rules. In a discipline where the civilian population is potentially as capable as the state of creating devastating weapons, the formulation and adoption of national or international policy and law takes time and consideration. This chapter provides a legal review of international law and ethics pertaining to cyber warfare and particularly self-attribution, and it strives to provide decision makers with a framework from which to make legal decisions about self-attribution.

The United States recognizes a series of international laws and conventions that relate to cyberspace and cyber warfare. First and foremost, the *U.N. Charter*, which specifies the basic rights of states and provides the criteria needed to engage in warfare, including cyber warfare.[41] Second, the *Tallinn Manual* outlines international law with respect to cyber warfare. These two documents and those documents and laws from which they are derived are acknowledged by the United States as a basis from which the country may wage war and respond to actions from others in the international

41 See *U.N. Charter*, Article 2 concerning sovereignty, dispute, and the use of force. See *U.N. Charter*, Article 51 concerning the right to self-defense.

community.[42] Therefore, these documents will make up the basis of this discussion.[43] Other documents included in this discussion are the *Law of War*, or *Law of Armed Conflict*,[44] the *War Powers Resolution*,[45] and *The Articles on State's Responsibility*.[46] The United States also recognizes just war theory in its conduct of warfare. Just war theory provides the criteria of *jus in bello* and *jus ad bellum* that need to be satisfied in order to engage in warfare.[47] In order to provide decision makers with better criteria for a self-attribution stance, the notion of just war theory needs to be included in the discussion. The following sections are the result of this research.

A. LAW AND ETHICS

During the last several years, the United States has struggled with the issue of cyberspace and how to deal with it as a nation. In March of 2013, James Clapper, the Director of National Intelligence, in his report to the U.S. Senate Select Committee on Intelligence, declared that the cyber threat had become the number one security concern to the American people at home and abroad.[48] This growing threat has prompted awareness and action at nearly every level of our government and across the international community. Detailed reports, mandates and laws have been developed and promulgated from the United Nations, the White House, the U.S. Department of Defense and nearly

42 The United States acknowledges international law as evidenced in multiple U.S. policies, most notably the Law of Armed Conflict and Law of War as prescribed by the Department of Defense.

43 See the Koh Speech made at the NSA in 2012, linking U.S. Cyber Law and *The Tallinn Manual*. See Schmitt's article on how the U.S. follows international cyber law in "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed."

44 *NWP 1-14M; The Law of War* is a naval publication that outlines the laws associated with armed conflict.

45 See *The War Powers Resolution* for the requirements of reporting between the executive and legislative branches of the U.S. Government.

46 See the *Articles on State's Responsibilities* for what is required of the state concerning its actions at home and abroad.

47 See Orend's *War* for discussions on Just War Theory, *jus in bello* and *jus ad bellum*; Farrell, Michael. *Modern Just War Theory: A Guide to Research*; Cook, Martin L. *The Moral Warrior*.

48 Cyber threats have been increasing in importance over the last decade, but in March, 2013 at the U.S. Senate Select Committee on Intelligence: Current and projected national security threats to the United States hearing by James Clapper (Director of National Intelligence) it became the number one threat to U.S. security at home and abroad.

every other major U.S. department. The release of *Homeland Security Presidential Directive-7* (HSPD-7) delineates government agencies' responsibility to safeguard key resources from cyber-attack.[49] It is possible that these critical infrastructures could be used to establish what a "use of force" cyber-attack would be defined as (tripwires that might illicit a response), and policy and law could be written on how to respond to an attack on these resources.

The creation of United States Cyber Command came about to protect against and deter those growing threats to U.S. security. With the creation of USCYBERCOM came the need for rules to guide the discipline of projecting power in cyberspace. In 2011, the *Department of Defense Cyberspace Policy Report*, to Congress, reads:

> As with all of the activities that DoD pursues in the physical world, cyberspace operations are executed with a clear mission and under clear authorities, and they are governed by all applicable domestic and international legal frameworks, including the protection of civil liberties and the law of armed conflict. (DoD Cyberspace Policy Report 1)

Many important documents link United States policy to both international law and the *Law of War* as pertains to cyberspace; two, in particular, are examined here. Harold Koh, State Department Legal Advisor, in his speech given at Fort Meade, Maryland to USCYBERCOM made several claims important to this thesis. Koh linked national cyber warfare policy to international law in his discussion, titled: "How do we apply old laws of war to new cyber-circumstances, staying faithful to enduring principles, while accounting for changing times and technologies?"[50]

The answer is that our national policy with respect to the United States' conduct in cyberspace is directly connected with and adheres to international law. This speech interestingly coincided with the release of the *Tallinn Manual*, which seeks to provide governance or rule sets over the actions of states in the conduct of cyber warfare.[51] Prior

---

49 HSPD-7, Critical Infrastructure Identification, Prioritization and Protection identify critical infrastructure and key resources in the United States for the purpose of securing them in cyberspace. This document was expanded in the Feb. 2013 PPD, "Critical Infrastructure Security and Resilience."

50 Koh, in his speech made at the NSA in 2012.

51 Michael Schmitt makes an excellent argument linking U.S. policy to the Tallinn Manual in: "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed."

to these comments, yet equally important, was the hearing of Lieutenant General Keith Alexander for his confirmation as Commander USCYBERCOM, where he stated that USCYBERCOM will be governed by the *U.N. Charter* and other international law principles as reflected in U.S. rules of engagement. He goes on to state that any use of force by USCYBERCOM will be congruent with international law, which helps link U.S. national policy to international law.[52] These documents and comments therefore provide an adequate linkage between international law and national policy.

International law may be considered to be the requirements and responsibilities that are levied upon the nation in its international conduct against and among other nations. This chapter focuses on the legal responsibility of the state and does not take into account the strategy a state is employing. If a state commits an illegal act under international law, it is responsible for its action under international law. If that state commits an illegal act and is caught, it has a responsibility under international law to address and if necessary redress the act. This is supported by the U.N. Security Council's right to enforce law through sanction or the conduct of warfare and by the numerous international tribunals that have been conducted to right international wrongs. However, does the state have a legal responsibility to disclose its operations in conjunction with its actions? The distinction and large problem is that the action must be attributable to the state in order for this onus of responsibility to stick. The articles on *Responsibility of States for Internationally Wrongful Acts* specifically includes attribution (the perpetrator must be exposed) as an element required for an act to be "wrongful."[53] This research finds that international law delineates no hard requirement to publicly acknowledge an action or require "self-attribution."

Just war theory may provide some traction for the theory of self-attribution, but not obligation. Just war theory provides the closest guidance available to point to a stance of self-attribution. The theory can be considered an international norm and is

52 See the remarks of Keith Alexander in his remarks, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command."

53 The responsibility of states is derived from *Articles on State Responsibility*: *International Law Commission, Responsibility of States for Internationally Wrongful Acts.*

incorporated into United States' national policy; consider Congress's role in declaring war, and the military's guidance through the law of armed conflict, both derivatives of the theory.[54] It serves to provide several beneficial indicators to leaders that the actions that they have taken or are about to take are morally and ethically justified. It does more than that as well. Just war theory can provide justification to the people of the nation and deliver an ultimatum to the adversary before the initiation of hostilities providing for a final moment to resolve an issue that is causing imminent threat of attack.[55] All of these ideas are found in preemption, and are addressed in just war theory.

Just war theory provides seven criteria that are required to be met before initiating a conflict. *Jus ad bellum* stems from these; they are not standardized and are subject to interpretation, but they are basically the same throughout most current writing. The theory is broken down:[56]

- Just cause: A conflict must be just, such as in self-defense, to protect innocents, or as a punishment for wrong doing.
- Legitimate or right authority. That the international political process was followed first. In this case, international law was consulted. In the United States, also that Congress must be consulted by the President (an unresolved conflict).
- Public declaration: That a state may conduct warfare only when made public to both its citizens and to the enemy state(s) resulting clearly in the reasons for going to war or conducting warfare. This provides a final moment for resolution between parties and makes it clear to the state being attacked, why the attacking state is fighting. This acknowledgement provides the authority for waging war.
- Just or right intention: Such as to limit war and restore a balanced state of affairs.
- Proportionality: Such as considering the casualties of war with respect to the expected results of the war. Are the benefits worth the costs, or is what it takes to win worth the cost of the outcome?

---

54 A look at the Law of Armed Conflict, the Army JAG's Deskbook includes an examination of how Just War Theory principles are applied to U.S. policy and decision making: *Law of Armed Conflict Deskbook*.

55 Martin Cook makes these points as part of his discussion in *The Moral Warrior*.

56 Farrell, Orend and Cook each provide similar explanations of just war theory in their works; these are presented as: just cause, public declaration, just intention, proportionality, last resort and probability of success.

- Last resort: Such that all other alternatives have been exhausted.
- Reasonable hope or probability of success: That mass violence without measurable impact or resolution to the conflict is futile.

National policy and law for going to war is codified in the *War Powers Act*. Accordingly, if the United States goes to war, the president has a responsibility to present his plan to Congress and announce to both the adversary and the American people as to the intentions of the president and the use of military forces. The act serves to limit the scope and duration of the introduction of military forces into hostilities.[57] Cyber-attack seems to fall under this policy but context is also important and therefore ethical considerations should also be taken into account. Law and ethics therefore should go hand in hand in order to better examine this problem. The next section will therefore examine principles and factors that decision makers should look at when deciding whether or not to self-attribute.

B. LEGAL CONSIDERATIONS

Several scenarios described in Figure 2 were identified in which cyber-attack between states might take place. The criteria used to advise on a stance of self-attribution are based on applicable national and international laws and just war theory, placing emphasis on the universal obligation of states to assume responsibility for their conduct and that of their organs in cyberspace. Organs of the state are defined as any parts of the government or those acting on behalf of or at the behest of the government.[58]

57 See the *War Powers Act* which seeks to limit the use of U.S. forces unless permitted by Congress.

58 The responsibility of states is derived from *Articles on State Responsibility: International Law Commission, Responsibility of States for Internationally Wrongful Acts*.

Decision Matrix for Recommending a Self-Attribution Stance

Type of Cyber Operation requirements/recommendations	**Legal Justification**	**Stance**
Cyber Espionage (all instances)	Not addressed in international law	Self-attribution is never required by law or Just War Theory (JWT)
Preemptive cyber-attack, prior to conventional attack	War powers resolution Just War Theory	Self-Attribution by international law, national law and JWT. Attribution falls on the affected state.
Offensive cyber-attack sanctioned under U.N. Security Council resolution	U.N. Charter Art 39 Tallinn Manual Rule 18	Self-attribution is not required by law or JWT, declaration is made through the U.N. as a proxy.
Offensive cyber-attack, valid military target, dual use object, civilian object.	U.N. Charter Art 2(4) U.N. Charter Art 52 Tallinn Manual Rule 10	A declaration of war should be considered and in some cases in effect is self-. attribution. However, self-attribution is not required for opening salvos or subsequent operations.
Self-defense cyber-attack against another state	U.N. Charter Art 51 Tallinn Manual Rule 13	Self-attribution is not required, but should be considered as a valid policy option.
Reprisal measure due to unlawful act by the enemy	Law of War Ch 6.2.3.1	Self-attribution is not required, but should be considered as a valid policy option.
Use of indiscriminate cyber-weapon in attack (all instances)	Conventional Weapons Convention Law of Armed Conflict Ch 9 Tallinn Manual, Rule 43	Consider self-attribution as a gesture to restore regional stability or through non-conventional channels to avoid regional conflict yet right the wrong.
Response cyber-attack due to intrusion, proportional, valid military target, civilian, dual use object	U.N. Charter Art. 51 Tallinn Manual Rule 9 Articles on State Responsibility (22,49-53)	Never required, but may be considered to justify the U.S. cyber-attack or to highlight the country being attacked as the original perpetrator.
Conduct of cyber-attack by state citizen acting at behest of state	Tallinn Manual Rule 6(9) Articles on State Responsibility (22,49-53)	Self-attribution is not required or recommended.
Failure to act to prevent a cyber-attack by citizens	Tallinn Manual Rule 6(4)	Self-attribution is not required, but may be considered to improve geo-political situation.

Figure 2. Decision Matrix for Self-Attribution

Interestingly, public declaration (as set forth in just war theory) may provide the closest guidance to point to a stance of self-attribution. If the United States goes to war, the President has a responsibility to present his plan to Congress and either a declaration of war by Congress is made to both the adversary and the American people or Congress may choose to limit the scope and length of the action. In certain situations where cyber-attack is the means of warfare, or cyber-attack is the opening salvo of a war, the attack could in effect be attributed to the United States at the point of declaration of war. In other words, declaring war and firing the first volleys through cyber-attack would, in effect, be attributing these attacks. These might be more overt cyber-attacks that would cause widespread outages or damages at wars onset, as covert cyber activities could go on prior to the declaration of war as well as after it without self-attribution. It must be clearly noted that this would be a policy decision and there is no requirement in international law, just war theory or national law that require it.

Of the many scenarios examined, none arise in which self-attribution is required in the sense that it is spelled out in law or obligated in theory. The research for this conclusion has explored many legal scenarios seeking to find ones in which self-attribution was a requirement. Finding none, it remains important to discuss why the requirement is absent. The lack of an obligation to self-attribute will impact strategy as equally as a hard requirement. The following scenarios demonstrate that law and ethics pose no obligations, but also examine why policy makers may consider different approaches.

1. Cyber Espionage

The conduct of cyber espionage between states is far more prevalent than open cyber-attack and warrants discussion here due to the highly covert nature of the operation. Espionage and cyber espionage are not addressed in international law vis-a-vis public declaration. Neither the *U.N. Charter*, just war theory, nor the *Tallinn Manual* provide details on the conduct of espionage and what is or is not legal. Cyber espionage by the United States for the purpose of intelligence gathering in all instances does not require self-attribution and there are no reasons why these actions should ever be

attributed. However, cyber espionage is becoming more and more intrusive, with many types of tools that can be left behind in the target system. It is questionable as to whether all of these tools fall under the espionage banner. Certainly, if any of them fall into the following section (those which may be considered acts violating international law) then self-attribution may be considered.

2. Preemptive Cyber-Attack Prior to Conventional Attack

In the case of United States conducting cyber-attack where the attack occurs without the presence of troops but in an area designated to become a combat zone, a conservative view of the War Powers Resolution could be taken.[59] In this case, reporting (that action will occur pre or post execution) to Congress by the executive (a matter of public record), and reporting to the public should occur. This does not mean that a specific operation is ever required to be publically acknowledged (just the war), but the following example provides an interesting twist on self-attribution.

Prior to conventional attacks into Libya in 2011, a cyber-offensive was planned against the Qaddifi regime in order to strike at his regime's military networks. This action was to be a series of cyber-attacks aimed at enabling allied forces to proceed into the nation unhindered by radar and air defense networks. One of the reasons it is believed that the cyber-attack was canceled was due to the War Powers Act requiring the president to notify Congress of the action. "Ordering a cyber-attack on Libya might create domestic legal restrictions on war-making by the executive branch without Congressional permission…require[ing] the executive to formally report to lawmakers when it has introduced forces into hostilities."[60] Though public acknowledgement may not have been the reason the attacks were called off, it nevertheless was a factor. This means that the cyber-attacks would be exposed and that self-attribution would occur. Overt cyber warfare was not conducted perhaps because this U.S. national policy would force self-attribution. It should be noted that the actual conventional attacks were very

59 See "The War Powers Resolution," U.S. Document (50 U.S.C 1541-1548), 1973.

60 See the article on the plan to cyber-attack Libya by Schmitt and Shanker: "U.S. Debated Cyberwarfare in Attack Plan over Libya."

public and fully acknowledged both prior to and during the action under the War Powers Resolution.[61] The President himself announced the action before and during the conflict. In this case, cyber-attack was affected by the War Powers Resolution, noting that self-attribution was not required to proceed with preemptive cyber-attacks resulting in war, but self-attribution would have in effect been achieved.

3. Offensive Cyber-Attack Sanctioned Under U.N. Security Council Resolution

An offensive cyber-attack is illegal under international law in most cases. The first example of where it could be held as legal is under the U.N. Security Council's purview. If a Security Council Resolution is passed and authorizes or mandates military action against another state and the United States decides that cyber-attack will be the means of attack against that state then the sovereignty of the nation under attack is not considered to be violated. The *Tallinn Manual* supports this claim. In this case, The United States, attacking via cyber operations may be conducting what would be considered an "armed attack" or "use of force" cyber-attack but not violating international law.[62] Under the umbrella of the Security Council's resolution, so long as the cyber-attack did not violate *jus in bello*, the attack would be justified and protected and no requirement would exist to self-attribute. Any offending state would have been authorized under the Security Council resolution to take the action and self-attribution of a specific nation would not occur.

4. Offensive Cyber-Attack

The *U.N. Charter* states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[63] From this statement, the *Tallinn Manual* provides supportive wording saying, "A cyber operation that constitutes a threat or use of force against the territorial integrity or

61 See instances of use of the War Powers Resolution: Libyan Conflict for the report to Congress.

62 The *Tallinn Manual*, Rule 18 and the *U.N. Charter*, Article 39.

63 See the *U.N. Charter*, Article 2(4).

political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[64] If an offensive cyber-attack or threat of cyber-attack is conducted by the United States against another nation and the targets are purely military in nature, but the attack is not sanctioned by the Security Council or executed for the purposes of self-defense, then the offensive attack is considered an act of war and is illegal under international law. This notion applies to dual-use objects (those used for both civilian and limitary purpose) and purely civilian objects (all objects that are not military objectives) as well.[65] This act not only violates the use of force, but also violates *jus ad bellum* regardless of the type of target.

These acts are all clear violations of international law. Cyber-attack with the intention of war (use of force, armed attack, or threat of) against another nation (regardless of the reasons) requires the United States to declare war, which according to just war theory and The War Powers Act publically acknowledges the action of going to war (but not the specific operation within that action). Strangely, in practice this may not be the case; this is an unclear contradiction, because the United States has not made a formal declaration of war in more than 40 years (the *War Powers Act* only being established in 1973). Further, the threshold of tolerance by the international community for considering cyber operations a use of force or armed attack is a high bar to date. It appears by all accounts that current cyber-operations continue to fall below the threshold of an armed attack, the level of activity which would trigger the right to self-defense. Nevertheless, the United States should consider, at least, self-attribution of a cyber-attack if the intention is to conduct war.

5. Self-Defense Cyber-Attack against Another State

Under international law and the law of armed conflict, the right to self-defense individually or collectively is an inherent right. The *U.N. Charter* and the *Tallinn*

64 See the *Tallinn Manual*, Rule 10.

65 See the *Tallinn Manual*, Rule 38 and 39. Also, see the U.N. report on the review of the NATO bombing campaign against the Federal Republic of Yugoslavia, in which it further defines dual-use objects under the *U.N. Charter*: "Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia."

Manual provide legal support to this for all attacks including cyber-attack.[66] The United States may respond in self-defense to any hostile act perpetrated against it through means of cyber-attack. So long as that cyber-attack is proportional in damage and no violation of international law occurred, then self-attribution need not be considered. Of course, national policy makers might consider the message that the nation wishes to convey, should we undertake cyber-attack as a matter of self-defense.

Context also plays a significant part. Consider if the United States responds in self-defense directly to a threat. In this case, *jus ad bellum*, the reason to go to war, is satisfied so long as the attack is necessary and proportional in response. However, if the attack causes significant collateral damage or non-military targets are targeted or destroyed, then the *jus in bello* principle of distinction between military and non-military objectives applies; proportionality might be violated.[67] If this attack was a large scale cyber-attack in self-defense, United States decision makers should seriously consider their responsibility and possible need to redress. In this case, the targeting and attack of civilian objects[68] (an unprovoked use of force even if accidently in self-defense) is illegal under international law, and though collateral damage is allowable, the effects of our weapons should be considered. In these cases self-attribution should be considered as a policy option.

6. Reprisal Cyber-Attack Measures due to Unlawful Actions by the Enemy

Similar to the above, under international law the right to self-defense is an inherent right. If in war, an adversary conducts a cyber-attack against the United States and that cyber-attack is considered a use of force attack against targets not allowed by the law of armed conflict then United States policy and international law allow for a response in the form of reprisal. Any immediate response is a reprisal against the adversary, even if it falls below the threshold of a use of force. Accordingly, LOAC dictates that the

66 See the *U.N. Charter*, Article 51 and the *Tallinn Manual*, rule 13.

67 See the *Tallinn Manual*, Rule 14.

68 Civilian Objects as described by the *Tallinn Manual* are all those objects that are not military in nature or used to support military operations. These objects may not be targeted.

authorized and justified reprisal, in response to an illegal act of warfare, should be proportional and the acts taken in reprisal should be brought to the attention of the enemy in order to achieve maximum effectiveness.[69] In this situation, in order to bring the action to the attention of the enemy, the reprisal cyber-attack should be self-attributed by the United States and conveyed to the adversarial leaders. The reprisal should be publicized or announced at, a minimum, to the adversary. In this case self-attribution is recommended but not required in order to communicate the action to the adversary.

It should be noted that in the case of cyber operations, simply stopping an attack may not meet the threshold of reprisal. Consider blocking IP ranges to stop an ongoing attack by an adversary. This means may not be considered a reprisal, but actively pursuing the culprit(s) and conducting operations against them to prevent the attack from happening again should be considered. In either case, communication to the adversary should take place especially if LOAC has been violated.

C. LESS OBVIOUS LEGAL SCENARIOS

1. Use of Indiscriminate Cyber-Weapons or Creation of Cyber-Fallout in Cyber-Attack

An indiscriminate cyber-weapon is defined as "the release of a weapon that cannot be directed at specific military objectives or limited in its effects" (Tallinn Manual 121). If the United States conducts a cyber-attack and makes use of a cyber-weapon that could be considered indiscriminate then this act is illegal (that it should not be done is obvious; that it may occur in the future still remains plausible). If a weapon used by the United States in a cyber-attack is incapable of being used in a way which enables a distinction to be drawn between military targets and civilian objects then it is inherently indiscriminate and therefore unlawful. Though the use of the weapon is illegal, only attribution of the perpetrator by a third party can trigger international action.[70] This problem is vexing in an environment where specially tailored and highly advanced malware can be released into the wild and attribution can be avoided. The targets may be

69 See *Law of War*, Chapter 6(3.2.1).

70 Again, *The Articles on State Responsibility*, Article 2, grapples with this issue, that an unlawful act must be attributable to the perpetrator.

very specific, and the malware may target them surgically, but as discussed in Chapter Two, the cyber-weapon more likely than not creates fallout, leaves traces of the malware that can be repurposed for infection of additional unsuspecting victims.

In this case the United States could consider a variety of options. If large scale destruction or damage was caused (economic impacts, power grid failures, etc.) the U.S. could consider self-attribution as way to correct the situation. Acknowledging the attack would have geo-political impacts, but if the fallout was regional and the attack was justified, then restoration of regional systems by the United States to restore stability could be a powerful and beneficial gesture. In another case, providing discrete information about how to defeat the worm or virus in question might also provide the same effect without self-attribution. Lastly, self-attribution could be done using private channels, between state actors as a way of not enflaming regional hostilities but restoring systems affected by cyber-fallout. There are many ways to maintain confidentiality of the attack or the ways and means of its delivery and still protect the region from indiscriminate effects.

2. Response Cyber-Attacks Due to Intrusions: Three Instances

Differing from the situations above concerning self-defense, a response cyber-attack is an attack in response to an intrusion into United States networks; the *Tallinn Manual* refers to this action as a countermeasure. The offender may or may not be conducting qualified cyber-attack (which would be considered a use of force or armed attack) but is conducting operations that meet a level of intrusion warranting response actions. The United States may take response actions in the form of cyber-attack against the target to stop the action (this could include the damage or destruction of the adversary's networks). In this first instance, the United States may conduct a cyber-attack against a military target found to be the source of an intrusion into U.S. networks. These cyber countermeasures are considered by international law to be legal and justified and not an instance of armed attack, regardless of the result.[71] Second, if the cyber-attack is in response to an attacking dual-use object then the effect is the same. Dual-use

71 See the *Tallinn Manual*, Rule 9 and the *U.N. Charter*, Article 51.

objects are considered targetable by the military.[72] Third, if the intruding object is civilian in nature and the United States attacks the object to stop the intrusion then the effect is different. It is possible that a state sponsored attack could utilize civilian objects in order to carry out the attack. In this case the rule concerning civilian objects does not apply. Civilian objects that are used to military advantage are permissible targets.[73] However, if the cyber-attack is not from a military source and not working on behalf of the state (a civilian hacktivist for example) a response of cyber-attack, with the goal of destroying the attacker, cannot take place, though lesser operations appear to be acceptable to stop the intrusion.[74]

In the situations above, the United States can order cyber-attack as a means to degrade, destroy or deter attacks only so long as they are proportional and the attacks fall under legal action within the scope of international law. It is recommended that no self-attribution stance be taken in these cases, as there is no requirement for it. However, the United States could use the situation as a means to justify its cyber-attack (as a response) or to highlight the blatant wrong doing of the perpetrator.

3. Conduct of Cyber-Attack by a State Citizen at the Behest of the State

Under *The Articles on States Responsibility*, states are responsible for their covert and overt actions and they are responsible for the actions of their private citizens who act on the states instructions. All actions of states that involve cyber-attack either by the state or by its citizens acting at the behest of the state are the responsibility of that state. These citizens are considered organs of the state if acting on its behalf and by virtue of

72 This is due to the same rule as under self-defense where dual-use objects are seen as valid military objects.

73 See the *Tallinn Manual*, Rule 38. Again, civilian objects can never be attacked legally under international law, even in cyberspace; *Tallinn Manual*, Rule 38. The only exception is if those objects are acting on behalf of the military, making them valid military targets; Rule 37 prohibits attacks on civilians, but an operation not qualifying as an attack is permissible. In this case, responses for defensive purposes may be legitimate.

74 Again, *Tallinn Manual* Rule 37 and 38 provide distinction between civilians working on behalf of the state and those not working on behalf of the state. This does not take into account terrorist actors that may be stateless.

the law of state responsibility.[75] If citizens of the United States conduct cyber-attacks for their government, then the United States Government is responsible for their actions. In this case, if Americans are conducting cyber-attack against other states at behest of their government, those actions of the United States citizen(s) may be considered unlawful under international law (depending on the effects of their attacks). Self-attribution is not required, but U.S. decision makers may weigh the benefits of acknowledgement.

4. Failure to Act to Prevent a Cyber-Attack by Citizens of the State (With Knowledge)

The United States bears responsibility under international law for attributable cyber-attacks of its citizens should they break international law. Therefore, should the state knowingly allow such an act (without efforts to stop it, or fail to prosecute post-act) it is illegal. This is especially true of citizens not acting at behest of the state.[76] International law states that if the citizen is committing cyber-attack and the state knows that the attack is imminent, ongoing, failed or completed and fails to take action to stop or redress the action then this is tantamount to condoning the action.[77] This is therefore illegal under international law. In this instance, the United States should strongly consider self-attribution and then take action to police its citizens to avoid geo-political friction.

D. SUMMARY

There are no concrete statements in international law requiring states to self-attribute their attacks on other states. Just war theory, does provide us with *jus ad bellum*, the criteria for going to war, which can lead us to a conclusion resulting in a decision to self-attribute. *The Articles on State Responsibility* demonstrate that a state is responsible for its actions whether it is caught or not. However, responsibility in cyberspace (as in physical space) for wrong is only challenged if the state is caught in the act or admits wrong doing. Only in a case where a declaration of war is required, and

75 See the *Tallinn Manual*, Rule 6 and *The Articles on State Responsibility*, Article 8.

76 See the *Tallinn Manual*, Rule 6.

77 See the *Tallinn Manual*, Rule 6.

thus attribution is assumed, does self-attribution come into play. This does not mean that self-attribution is not a serious policy issue that merits attention given the legal scenario. The lack of requirements or obligations in law and ethics to self-attribute cyber-operations and attacks creates opportunities for applying and leveraging strategy. In the end, self-attribution will be more a choice dependent on geo-politics and national interest and less on international law or norms.

The potential of cyber-attack to transcend national boundaries with speed and ease makes the issue an international one. The potential of that cyber-attack to be launched from nearly anywhere by state or non-state actors mandates the need for international response and control, hence the *Tallinn Manual* and the power granted to the U.N. Security Council. This idea of a system of international norms is incorporated in the United States' policies concerning conventional, nuclear, biological, mine and cyber warfare and is supported by treaty ratification, the *U.N. Charter*, the *Law of Armed Conflict*, the *Articles on the Responsibilities of States* and most recently by the laws set forth in the *Tallinn Manual*. Just as an unlawful conventional attack or nuclear attack may not be hidden or covert in the eyes of international law due to their overt natures, neither should cyber-attack regardless of it covert nature. Until the emerging cyber battlefield is better agreed upon under international law and norms materialize concerning how states must conduct themselves in cyber-war, self-attribution will remain a choice.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. STRATEGIC OPTIONS FOR SELF-ATTRIBUTION

When discussing the strategy of self-attribution, context is important. This chapter will examine how strategy and timing may influence the decision to self-attribute a cyber-attack. Perhaps the choice to conceal one's action avoids certain war. Perhaps taking responsibility for an action provides currency for diplomacy. Perhaps the use of a cyber-weapon is for purposes of brandishing. The launch of a cyber-weapon in an offensive attack as a means to communicate our possession of the weapon is an extreme notion. The risks associated with developing and using weapons that have the potential for massive and widespread destruction are extensive, and thoughtful intelligent strategy must be employed to oversee their possession and use. Cyber-weapons could be considered the next round of such weapons.

The United States has formulated and promulgated many documents to outline its future strategic security posture; four stand out in terms of cyber-security. United States National Security Strategy (NSS) lays out the broad strategy that the nation will pursue. The Comprehensive National Cybersecurity Initiative (CNCI) outlines goals designed to secure the United States in cyberspace. The Homeland Security Presidential Directive (HSPD-7) identifies critical resources and key infrastructure (CRKI) that if attacked by cyber-means would constitute catastrophic risk to national security. The United States International Strategy for Cyberspace (US-ISC) seeks to build international norms, forge partnerships and emphasize the nation's right to unilateral and collective self-defense. These four documents highlight the seriousness of cyber threats to the nation and treat the nation's public and private digital infrastructure as a strategic national asset and warfare domain.

This chapter examines four strategic conditions under which the United States might consider a stance of self-attribution. Each of these conditions supports the nation's national security strategies of securing cyberspace and deterring foreign and criminal aggression in cyberspace. They link to the NSS, CNIC, HSPD-7 and US-ISC in order to demonstrate how self-attribution might advance national security interests and objectives in cyberspace. Figure 3 lists the four strategies and provides decision guidance for each.

The first reason for self-attribution is to communicate our capability to the adversary. Demonstrating our cyber capability can provide several benefits such as exposure of the adversary's weakness, exhibition of our strength, or perhaps simply demonstrate that our capability exists. Second, self-attribution can be used strategically to communicate willingness or intent to use cyber-weapons both offensively and defensively. This may entail the creation of a policy of guaranteed proportional response to an attack or intrusion that is public and offers the option of self-attribution as a means to communicate intent to the enemy. Conversely, the U.S. may want to pursue policies to demoralize or intimidate; conducting a cyber-attack to attrite an adversary's resources or morale could achieve these policy goals. Self-attribution of an intrusion into adversary networks will force him to expend resources in attempts to counter. A more invasive intrusion or attack could elicit significant countermeasures which could harm his national economy or damage morale. Third, self-attribution can be used as a means of building deterrence by self-attributing a combination of capability and intent. Finally, and conversely, a posture of self-attribution could be used to set things right, restore systems to operational status or redress grievance or damage. The remainder of this chapter discusses each of these four strategic conditions.

A. SELF-ATTRIBUTION TO COMMUNICATE CAPABILITY

Capability can be communicated to an adversary by self-attributing a demonstration of that capability. US-ISC explicitly expresses the U.S.'s right to self-defense in cyberspace, either unilaterally or collectively.[78] If a cyber-attack is considered as a means of self-defense, then international public disclosure of our capability can provide our adversary with the foreknowledge that we possess the means to defend ourselves. Perhaps a strategy of forward presence in cyber space is sought. In this case, self-attributed public demonstration of capability reminds our adversaries that we are out in the domain preparing and training to our capabilities. If we choose a strategy of pursuing and isolating rogue nations, private self-attribution of a cyber-operation (between two parties or a small group) can tell the rogue nation that we are watching and

78 The US-ISC discusses the basis for norms, citing the right of self-defense.

have capable means of defeating them. If our strategy is collective security, among nations, then our capability in combined operations also merits disclosure, or self-attribution. One example may include exhibition of cyber-weapons publicly in a test environment.

A National Cyber Range is currently being developed in order to test the effectiveness of cyber tools.[79] This cyber-range could have a public aspect, one idea could be the creation of a Joint/Combined Cyber Exercise Area (CXA)[80], just as the demonstration of new surface-to-air-missiles or radar systems serve to demonstrate conventional weapons' and tools' capabilities. Such a program would officially tie the possession of cyber capabilities to USCYBERCOM and communicate their existence without necessarily disclosing their interior construction, command and control or deployment methods. The program would, however, demonstrate the tools effectiveness through employment in an environment constructed to be sandboxed (an environment for testing software without allowing harm to networks) and publicly available for viewing.

A CXA could be an environment where both offensive and defensive capabilities could be tested or displayed. As with conventional and nuclear tests, these could be publicly witnessed. Success and failure could be announced, avoiding the need to downplay leaks or revelations. As the CXA was developed, joint (J-CXA) and combined (C-CXA) exercises could be conducted to demonstrate and hone maneuver and targeting. This type of activity would demonstrate not only the capability and existence of various cyber weapons, but also the relationship of nations participating in the exercises. A demonstration of maneuver warfare among allies could help fulfill the US-ISC's requirement to develop means and methods of collective self-defense and security to deter and defend against state and non-state actors.[81]

---

79 See DARPA's white paper "The National Cyber Range" on the development of the NCR for testing and collaboration.

80 DARPA describes the current National Cyber Range as useful for advanced cyber research, development of new capabilities, analysis of malware, cyber training and exercises. The range could be used to exercise military maneuver in joint and combined exercises. see: <http://www.darpa.mil/NewsEvents/Releases/2012/11/13.aspx> for more information on DARPA's plans.

81 The USISC highlights the need to work with allies to promote collective self-defense.

In his work, "Brandishing Cyber-Attack Capabilities," Libicki discuss the reasons to demonstrate one's weapons. He shows how brandishing cyber weapons can support threat making or counter the threat of the adversary (Libicki 1-4). Public acknowledgement and demonstration in a test environment can support these strategies and others. If cyberspace is to be considered a new domain (both public and private) and our goal is to secure it through dominance or primacy, then demonstrating our capability is a key to supporting this goal. Just as demonstrations of nuclear weapons confirmed offensive capabilities and testing of anti-ballistic missiles confirmed defensive capabilities, demonstrating cyber-weapons can achieve the same ends. However, the United States also strives to partner with its allies to achieve security and can use these exercise areas as means to demonstrate and achieve collective security between nations.

Communicating capability through demonstration requires that certain criteria are met before engaging in the activity. Policy and decision makers should consider the following:

- When does self-attribution through public display of a weapons test make sense?
- Is there reasonable expectation that the display will have the desired effect on the adversary?
- Is there reasonable expectation that the demonstration will send a signal to the appropriate adversarial leadership?
- Will demonstration have a negative effect, such as escalation or sparking of an arms race?
- Is the cost of self-attribution through these means worth the expected benefit?

Decision makers should also consider timing and legal questions. Self-attribution of cyber capabilities in this case should occur prior to or concurrently with action against the adversary and perhaps used as geo-political capital to prevent conflict. However, a demonstration of a capability might expose the United States to a situation where its use, if considered first-strike, preemptive, indiscriminate or accidental might draw attention internationally since attribution could be more easily established.

This approach will likely be most effective against state actors and less effective against non-state or individual actors that are outside of the diplomatic arena. Such an

approach can directly link efforts to national security needs and goals outlined in the *United States International Strategy for Cyberspace.*[82] If there is reasonable belief that using the national CXA can support strategies such as collective security and communicate to potential adversaries that a cyber-attack could be met with a sophisticated and capable response then the demonstration should be considered.

Decision Matrix for Recommending a Self-Attribution Stance

Type of Cyber Operation requirements/recommendations	**Strategic Support**	**Stance**
Demonstration of capability to communicate ability to defend unilaterally or collectively	Supports National Security objectives outlined in US-ISC	Utilize national Cyber Exercise Area (CXA) to demonstrate capability of cyber-weapon and capability of joint and combined force in cyber-maneuver warfare. Timing will be in advance of conflict.
Doctrine developed to create redlines and guarantee response. Self-attribution to demonstrate U.S. Strength or expose adversary weakness to communicate willingness or intent.	Supports National Security objectives outlined in US-ISC, CNIC, and creates redlines in support of HSPD-7	Use doctrine to demonstrate willingness to. respond. Requires the creation of redlines. Use cyber-operations to attack/penetrate adversary infrastructure to elicit response. Timing depends on strategy.
Self-attribution as a means of forwarding deterrence policy	Supports National Security objectives outlined in CNIC and US-ISC concerning building deterrence programs and deterring malicious activity.	Use a combination of demonstration and the communication of intent and willingness through self-attributed cyber-operations and doctrine to deter adversaries actions in cyberspace. Timing will be variable.
Self-attribution to set things right	US-ISC and Cyberspace Policy Review calls for strategy to build and establish norms in cyberspace.	Use self-attribution as a means to set things right in order to assist in establishing norms of states' conduct with respect to the use of cyber-weapons. Timing depends on strategy

Figure 3. Decision Matrix for Self-Attribution

B. SELF-ATTRIBUTION TO COMMUNICATE WILLINGNESS OR INTENT

Self-attribution may be used to communicate willingness or intent to an adversary. Defense of the homeland is a consistent theme in national discourse and an overarching tenant of *National Security Strategy*.[83] If the United States is to pursue ways

82 US-ISC discussed building and strengthening partnerships through the development of means and method of collective self-defense, a goal that the CXA could help achieve.

83 *National Security Strategy* outlines several goals, the first of which is the security of the U.S. homeland and its citizens.

in order to secure cyberspace, we must be able to effectively communicate our intentions to perceived and real adversaries. It terms of defense, the U.S. might communicate its intolerance for intrusion; that it will be met with resistance and if necessary, retaliation. In terms of offense, the U.S. may use direct or indirect aggression, perhaps to win hearts and minds or demoralize war fighters and maybe to merely show a level of invasive intrusion.

Consider two scenarios, internal doctrine that outlines defensive intent (what we will definitely do) and external signals (what we are able to do) to demonstrate willingness to act. First, self-attributed cyber-operations in response to cyber-attack or cyber-intrusion could be met with guaranteed response. Doctrine could be developed that states a cyber-attack will be met with a counter cyber-operation in a proportional response aimed at stopping the attack, preventing additional attacks or even destroying the capability. In this case, self-attribution of the response attack would relay to the adversary that the United States will respond and not tolerate such action. Second, self-attribution to communicate willingness to use cyber-weapons could take on several forms. In the case of warfare, exhausting an adversary's resources or negatively affecting morale through attrition could be a powerful tool. Cyber-attack or cyber-exploitation may be conducted against an enemy to make that enemy appear weak, or to make the United States appear strong. This is likened to sending a message to the leaders of the adversary. Self-attributing a cyber-operation to the enemy's leadership, even subtlety, can prove an effective strategy to communicate the United States' willingness to use cyber-weapons.

1. Doctrinal Case

United States International Strategy for Cyberspace affirms the right to self-defense as: "Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace" (US-ISC 10). The document further reserves the right to use all means necessary to defend the

nation.[84] Yet, how do we officially tie a threat or aggressive act in cyberspace to national security; an armed attack or act of war? The development of response doctrine could achieve the desired effect.

Consider the critical infrastructure as defined in HSPD-7. HSPD-7 defines what critical infrastructure in the United States is vulnerable to cyber-attack and designates agencies responsible for securing each. Critical U.S. infrastructure is defined as: Agriculture, Public Healthcare, Water, Energy, Finance, Monuments, Industry and Defense.[85] Redlines or tripwires could be established at the critical infrastructure laid out in this document. A doctrine of immediate and guaranteed proportional response, which includes retaliatory cyber-attacks, could be adopted to specify how the United States will respond should any of the nation's critical infrastructures be penetrated or attacked. [86] This declaration of critical cyber-infrastructure would link thresholds to national security objectives (defense of the nation) in order to deter attacks and create trip-wires (redlines), producing a more accurate definition of what a use of force or armed attack would be. In turn, this doctrine could officially tie a threat in cyberspace to national security and define a cyber "act of war" or "armed attack," linking the strategy directly to national security objectives.

Communicating intention through doctrine and the creation of redlines has both benefits and drawbacks. Policy and decision makers should consider the following:

- Drawing redlines can be a powerful deterrent, however, a redline implies that crossing the set line will incur response. Failure to act could be construed as weakness and negatively impact foreign policy goals.
- Intrusion falling below the threshold of armed attack or unwarranted aggression might warrant response crafted to be aggressive against attackers, yet also remain below the threshold of declared war; like surgical strikes of proportional response.

---

84 Self-defense is reaffirmed as a right for the United States. National Security Council (U.S.), and United States. Executive Office of the President. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." p. 14.

85 Derived from "HSPD-7, Critical Infrastructure Identification, Prioritization and Protection."

86 Cordseman discussed the need to develop clear response doctrine in the conclusion of his work, "Cyber-Threats, Information Warfare, & Critical Infrastructure Protection." He discussed the clear need to distinguish between what is a nuisance and what may need massive retaliation in general terms; this chapter builds on that idea and lays out the lines that might be developed to decide on response.

- There would be no need to delegate authority to release of cyber-weapons below the executive office, since response would be at the time and place of our choosing.
- If the adversary's intrusion or attack was of sufficient sophistication or severity it could warrant response or simple "denial."
- The doctrine must be public, (or delivered privately the adversary) in order to effectively communicate the message to potential adversaries.
- Allies, such as those in NATO should be consulted when making declarations which might impact collective security agreements.
- The action of creating redlines could be seen by some nations as an escalatory practice causing tension in foreign policy.

The idea of self-attribution through doctrine implies public acknowledgement prior to engagement and therefore advanced timing. What constitutes a cyber-attack against the United States becomes more stringently defined. The adversary is notified of what will happen should the redline be crossed and, therefore, should the United States conduct a retaliatory response, attribution will be assumed. International law states self-defense is an inherent right and what triggers self-defense is defined, so United States actions triggered by this doctrine would be legal under international law. This approach would likely be effective against state actors. It could encourage those states lenient against malevolent non-state actors operating within their borders to act more aggressively to curb their illegal cyber-activities. In this case defense and deterrence value could be achieved.

2. External Signals Case

In this case, a cyber-operation may be conducted against the adversary's networks to disrupt or degrade those networks in order to demonstrate willingness. Self-attribution could be used to tell the adversary that the United States has the ability and means to attack, but not disclose the ways or means that the exploitation was conducted. In essence, "we have control of your networks; you are powerless to stop us." Libicki addresses nearly the identical issue: his "hack in and leaving a calling card" idea (Libicki viii). He claims that we need to choose between making the adversary look weak and demonstrating our strength. In order to do either he surmises that we must demonstrate the capability repeatedly in order to be effective and that an effective campaign may

affect the enemy's choice to pursue war.[87] In support of these theories, self-attribution to send signals can provide an enhancement of this idea, eliciting several benefits. First, a feeling of being powerless can be detrimental to the morale of the adversary. A strategy of demoralization only starts with the adversary's military; it can have drastic effects on public opinion. Uncertainty, through indirect aggression, such as documented cyber intrusions, could as a result eat at the strength or legitimacy of a government or régime. Second, the adversary will be required to expend considerable resources to defeat the capability. This equates to an expenditure of in money, time and resources which the adversary may not have in abundance. This then is an effective means of attrition, especially if the adversary has no guarantee of success against the intrusion.

A brief examination of incidents reports to US-CERT shows that between 2006 and 2012, reported incidents (Federally reported incidents of malicious code injection or unauthorized accesses to information) rose by 782 percent or nearly 10,000 incidents per year.[88] Contrast that with spending patterns; on a nearly identical linear rise of more than a billion dollars a year; the U.S. has spent billions of dollars combating cyber-intrusion and attack, with 2014 spending predicted estimates topping 14 billion dollars.[89] This shows how malicious cyber-activities inside a nations network can lead to changes in policy and attrition of resources; here dollars used to defend networks. It is important to note that these are only reported Federal attacks and Federal dollars; the private sector is affected as well. This pattern appears to demonstrate that forcing a nation to defend assets that it thought secure can lead to a tremendous expenditure of resources that may have been spent elsewhere. Eliciting such a response in other nations through self-attribution of a cyber-operation is possible.

Communicating willingness through cyber-operations can be used to achieve strategic goals. Policy and decision makers should consider the following:

---

87 Libicki, Martin C. "Brandishing Cyber-attack Capabilities." p. vii-ix.

88 From: "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented."

89 See VanRoekel's article: "Federal Information Technology Budget Priorities 2014."

- Does it make sense to tell the adversary that you are present on their networks? Will the introduction of a threat be counterproductive to the strategic goal?
- Burning a cyber-capability may occur (exposure of a capability may be enough to allow the adversary to counteract it). Will there be sufficient residual access if the attributed capability is defeated?
- If the goal is to achieve presence in a sensitive network, will the message be conveyed to the appropriate leadership?
- Will the adversary "feel" the desired level of pain or anxiety that will elicit the desired reaction: defense, dispirit or weakness?
- If the nation being attacked or threated has considerable resources, will their use of resources to defend be counterproductive? Is the cost of maintaining presence significantly smaller than the cost to the adversary?

Self-attributing a cyber-operation against an adversary to communicate willingness can take advantage of timing. Exposing the operation to the adversary after the operation is complete will likely elicit the desired action. The enemy will be forced to take measures to secure his networks. Used as a precursor to war, this can be a powerful force multiplier and a blow to the adversary's morale; if the enemy realizes that his air defense systems are compromised, then he is uncertain his weapons will work to defend his area of operations, perhaps leading to more decisive victory or faster termination of war. In terms of legality, things are less clear. Cyber-attack, as defined in the *Tallinn Manual*, causes death, damage or destruction to physical objects and is not permitted under international law, unless in self-defense or under U.N. Security Council authority. Unintended collateral damages fall into the cyber-attack definition.[90] Cyber-operations conducted under the guise of espionage or not rising to the level of "attack" as defined in the *Tallinn Manual* are less likely to draw scrutiny. However, launching a preemptive operation or attack for the purposes of showing willingness to attack could appear as an act of aggression and therefore decision makers must carefully weigh the expected outcomes and benefits against the possibility of causing a wider conflict.

This strategy can forward U.S. strategic initiatives outlined in U.S. CNCI. Initiatives supporting the development of better counter-intelligence and deterrence

90 See the *Tallinn Manual*, Rule 30.

strategies could include demonstrations of willingness against adversaries that are penetrating U.S. networks and conducting cyber-operations there.[91] As discussed, the U.S. is already spending billions to secure government networks. Actions in the form of cyber-operations to communicate willingness against the adversary could certainly be justified as proportional responses to invasive threats to our national security.

C. SELF-ATTRIBUTION TO FORWARD CYBER DETERRENCE

A combination of demonstrating capability with intent and willingness can create a powerful deterrence model. The nation's *National Security Strategy* seeks to strengthen deterrence strategy in cyberspace primarily in support of defense of our economic and defense structures.[92] Using self-attribution through strict doctrine, public demonstration or attributed operations could signal other nations that the United States will not tolerate acts of aggression or invasive intrusion against its networks. One example to achieve these strategies could be cyber-attack in a proxy warzone. The United States has fought several wars in which the adversary was supported militarily by a tertiary nation (with whom the U.S. was not at war). Recent U.S. involvement in Libya and Afghanistan where Iranian influences are confirmed can demonstrate this point. In these cases, demonstrating attack capabilities against the primary adversary in the war zone demonstrates capability and intent to non-participating adversaries, for example Iran, in a setting where attribution is implied. A show of dominance in cyber-capabilities can be a powerful deterrent to those who may wish the United States harm.

Similarly, where the United States is providing the military support, such as in Syria, which is being aided by Russia. Self-attribution of a cyber-attack against Syria, in support of rebel allies, would be effective in sending the message to a third party without actually engaging them that the United States has the capability, intent or both to conduct cyber-attacks. Martin Libicki, in his work "Brandishing Cyber Capabilities," discusses the "teeth" a deterrence policy has and that it is based on the willingness a state has in

91 Issues six and ten deal with counter-intelligence and deterrence of adversaries in cyberspace: "The Comprehensive National Cybersecurity Initiative."

92 The White House recognizes the difficulty of deterring sophisticated adversaries and seeks a strategy to bolster and renew deterrence models, see: The White House, "National Security Strategy 2010."

enforcing its established redlines and the greater its capacity and capability to strike (Libicki 3–4). A strategy of indirect aggression could satisfy such a policy in a non-escalatory environment. Combining demonstration in willingness, intent and capability in careful and meaningful ways can achieve the teeth that Libicki speaks of and perhaps do so in a way that does not spark escalatory behavior.

Working to achieve deterrence through self-attributed cyber operation has benefits and drawbacks that need to be considered:

- Demonstrating capability and intent through a third party suggests avoiding direct confrontation with the intended recipient of the message. This may prove an effective way of deterring more powerful adversaries without having to engage them militarily.
- Deterrence policy must be seen as serious, but redlines need to be carefully crafted, and demonstrations need to be carefully conceived so as not to spark undesired escalation or conflict.

Forwarding cyber deterrence through self-attribution strategies is a long-term strategy that requires considerable planning and careful timing. As discussed in the above sections, demonstration of capabilities can occur in a CXA or a current war zone, communication of intent should be attributed early to establish tripwires, and communication of willingness can occur at the time and place of the decision makers choosing. Together, these techniques can be combined to create a firm deterrence stance and support national security objectives of building enduring deterrence strategies and programs that will deter hostile and malicious activity as outlined in both the CNIC and US-ISC. These methods combined might be effective against both state and non-state actors, perhaps encouraging offending states to better police their intelligence agencies and populations.

D. SELF-ATTRIBUTION TO SET THINGS RIGHT

Last, self-attribution may be used in order to right a wrong done by the United States. This thesis has taken into account the need for policy makers to carefully weigh their options when engaging in cyber warfare for both legal and strategic reasons. It has also stressed how important it is for a state to take responsibility for the actions it takes in cyber warfare. Furthermore, this thesis has shown how just war theory and the

Responsibilities of States have become ingrained in both national policy and international law. It therefore makes sense to consider public acknowledgement of cyber operations taken by the United States that cause inadvertent or deliberate damage, collateral or otherwise. Responsible behavior in cyberspace is outlined in *U.S. International Strategy for Cyberspace* as the central goal of our strategy and a primary national interest. Therefore, this strategy can directly support this notion.

Many scenarios could prompt self-attribution to set things right. The United States could conduct a cyber-attack with a weapon that has inadvertent or secondary (intended or unintended) indiscriminate effects. Accidental release of a cyber-weapon could occur, or inadvertent collateral damage might occur from the weapons use. In more serious cases, covert actions that caused serious damage could be leaked internally or attributed to the United States by the recipient. Most cyber weapons are sophisticated in design, with highly pointed effects. Some are designed for a single purpose, others for one time use and then deletion, yet second and third order effects are much harder to determine with any certainty. Cyber fallout is a real possibility that should be taken into account during the planning process. Even when an attack is legal and justified, consideration should be given to this option.

Decision makers will struggle with this option, as self-attributing a wrongful or even illegal act could harm the United States in foreign policy. Some of the questions and issues to consider include:

- Was the effect of the cyber-weapon outside of the expected outcome?
- Did the use of the cyber-weapon violate the law of armed conflict?
- Could self-attribution of the attack be useful in foreign relations? Will righting the wrong help to make a bad situation better?
- Would possible second or third-party attribution or leaking of the action by an insider be more harmful to the U.S. than open, self-acknowledgement?
- Can self-attribution be conducted privately between the U.S. and the affected party? Direct diplomatic intervention at the state level without wider public acknowledgement could save face with both parties.
- Can redress take place covertly, such as the removal of malicious software from adversary machines without public knowledge?

How do policy and decision makers keep a bad situation from getting worse? For example, in 1960, after repeated denials, President Eisenhower had to admit CIA involvement in Soviet overflights for intelligence gathering. The U-2 spy plane incident was an avoidable embarrassment. Consider the recent leaks by Edward Snowden concerning the National Security Agency's programs.[93] Perhaps blanketed denial of U.S. cyber capabilities isn't the answer in all situations. Self-attribution either publicly or privately could be an answer to these problems. International law, the Responsibilities of States and just war theory all support this notion, that states are responsible for their actions and that redress of wrongs is a state's responsibility. Timing of such redress is always post-action and as the saying goes: "bad news doesn't get better with time".

Obviously there are endless geo-political minutia to consider, but self-attribution to set things right is a valid strategic option. This strategy might be useful, not only in achieving our national interests, but also in limiting damages from our cyber activities to our international policy and reputation. It further can assist in establishing norms in cyberspace. The recent *U.S. International Strategy for Cyberspace* stresses that "We will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace" (US-ISC 8). Likewise, the White House "Cyberspace Policy Review" highlights the need for *norms* in the international community regarding territorial jurisdiction, sovereign responsibility, and use of force (20). Self-attribution to set things right can be a strategy to establish norms of responsible behavior. If so, leadership in responsible behavior should be incorporated into our decision making; this strategy can support this notion.

93 Edward Snowden is a former contractor of the NSA who leaked a large number of classified documents to the media.

V. CONCLUSIONS

Through the course of history, leaders have struggled with providing security to their people. To these ends, strategies have been developed to achieve that security in and among nations. War, a violent and overt tool of strategy has been one traditional way of settling differences between nations. Attacking one's enemy to ensure one's own security is not unusual, but over time has come to be viewed as uncivilized and banned to the extent that the international community can enforce it. Norms emerged from this order. Cyberspace however presents a new domain and challenges those norms, particularly because of the attribution problem. Where the use of conventional and nuclear weapons is in most cases tied to the identity of the user, that bond is uncoupled in cyberspace. This domain is one where nations have the opportunity to attack with low degrees of attribution and therefore low risk of reprisal. This applies equally to just and unjust wars and actions.

When the decision is made to conduct cyber-attack, men and women of our government must deal with the results of our attack. A decision must be made either before or after the attack as to a self-attribution stance; to tell the adversary that we conducted the attack or to keep the attack covert. Decision makers may be faced with situations where United States strategy and policy point one way and international law the other. Law tells us what we may and may not do. Strategy is the method in which we will achieve our national interests. However, in cyberspace there are no legal restraints on this decision. This thesis has shown that self-attribution of cyber-attack is not required by international law. For the United States, this means that public acknowledgement of a cyber-attack may ultimately only "legally" come in the form of a declaration of war, unless it is in our strategic interest to do so. This claim is based on the requirement of the Executive and Congress as set forth in *War Powers Act*, and supported legally by the *Tallinn Manual* and the *U.N Charter* and ethically through just war theory.

A. NATIONAL INTERESTS AND INTERNATIONAL NORMS

As cyber capabilities mature and future generations of political and military leaders are faced with decisions regarding self-attribution, they too must consider the impact to the international community. The new domain of cyberspace interconnects us in ways that may surpass those of physical space. Nations will clash in new and unexpected ways and private citizens will realize unprecedented power, as the price to enter the cyber-arena is driven lower and lower. Norms in the international politics of cyberspace will materialize, and creating those norms requires leadership, cooperation and some level of transparency. Self-attribution of attacks can drive the establishment of these norms among nations.

New ideas will have to be developed to forward norms in cyberspace, future work might consider the following such ideas. First, treaties guaranteeing no "first use" of cyber weapons could be established. No first use would establish what cyber capabilities would be considered off the table in the conduct of nations in cyberspace. Alternatively, the international community could agree that all nations take greater responsibility for the actions of their citizenry in cyberspace. This action places the onus of responsibility and policing on the nation and perhaps renews enforcement options in the international community. In any case, the international community must come together to answer basic questions regarding "use of force" and "armed attack" long before these norms can effectively be established.

B. SUMMARY

In conclusion, it has become apparent that deciding on a self-attribution stance is as much an art of foreign policy as it is an art of war. This thesis has examined the question; under what strategic and legal criteria should the United States publicly acknowledge responsibility for a cyber-operation? From the perspective of international law, there are no hard requirements to self-attribute an action in cyberspace, even in the most extreme cases. Strategically, self-attribution has a valid place in building deterrence models and in foreign policy as another tool of soft power or reconciliation. Both cases

should incorporate thought on the ethical use of cyber weapons, as what a nation may do legally or illegally to achieve its national aims may well have unintended consequences that will have to be reconciled.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"Bots and Botnets—A Growing Threat." *Symantec.com.* Symantec Corporation. 2013. Web. 2 Oct. 2013. http://us.norton.com/botnet/.

Breeden II, J. "Hackers' New Super Weapon Adds Firepower to DDOS." *GCN.com.* GCN Technology. 2012. Web. 3 Oct. 2013. http://gcn.com/articles/2012/10/24/hackers-new-super-weapon-adds-firepower-to-ddos.aspx.

Clapper, James. Hrg, Senate, 112-481. "Current and Projected National Security Threats To the United States." (2012). Web. 08 Aug. 2013. http://www.fas.org/irp/congress/2012_hr/threat.pdf.

Clark, Collin. "DoD Unveils New Cyber Strategy; Cartwright Urges Shift from Defense." *Breakingdefense.com*. Breaking Media Inc. 14 Jul. 2011. Web. 07 Feb. 2014. http://breakingdefense.com/2011/07/dod-unveils-new-cyber-strategy-cartwright-urges-shift-from-defe/.

Clark, David, D. "Untangling Attribution." *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. 1.2 (2010): 25–40. Web. 10 Aug. 2013. http://cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf.

Clark, David D., and Susan Landau. "The problem isn't attribution: its multi-stage attacks." *Proceedings of the Re-architecting the Internet Workshop*. 11 (2010): Web. 18 Aug. 2013. http://dl.acm.org/citation.cfm?id=1921247.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco, 2010.

"The Comprehensive National Cybersecurity Initiative." The White House. The White House, 2009. Web. 22 Jan. 2014. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Cook, Martin L. *The Moral Warrior*. Albany: State University of New York Press, 2004.

Cordesman, Anthony H. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland*. Westport, CT: Praeger, 2002. 167–179.

"Cyber Strikes a 'Civilized' Option: Britain" n.a. *Technology Inquirer*. Agence France-Presse, 3 Jun. 2012. Web. 12 Sep. 2013. http://technology.inquirer.net/11747/cyber-strikes-a-civilized-option-britain.

"Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." *United States Government Accounting Office*. 2013. Web. 15 Dec. 2013. http://www.gao.gov/assets/660/652170.pdf.

"Department of Defense Cyberspace Policy Report." *Defense.gov.* Department of Defense. Nov. 2011. Web. 01 Nov. 2013. http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

DiMeglio, Richard P., Sean M. Condron, Owen B. Bishop, Gregory S. Musselman, Todd L. Lindquist, William J. Johnson, Andrew D. Gillman, and Daniel E. Stigall. *Law of Armed Conflict Deskbook.* Charlottesville, VA: United States Army Judge Advocate General's Legal Center and School, n.d.

Doyle, Jeff. "Understanding Dual-Stack Lite." *Network World.* 22 Oct. 2009. Web. 2 Oct. 2013. http://www.networkworld.com/community/node/46600.

Executive Office of the President "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." *The White House*.. 2011. Web. 10 Nov. 2013. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Farrell, Michael. *Modern Just War Theory: A Guide to Research*. Lanham, MD: Scarecrow Press. 2013.

"Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia," Section 4-37. Rep. *United Nations*, 13 Jun. 2000. Web. 15 Jan. 2013. http://www.icty.org/sid/10052.

"Flame Cyber Weapon Fact Kaspersky Lab U.S." *Kaspersky Lab United States*. Kaspersky Lab, n.d. Web. 15 Sep. 2013.

"Flame." *Endpoint, Cloud, Mobile & Virtual Security Solutions*. Symantec, n.d. Web. 10 Oct. 2013. http://www.symantec.com/security_response/writeup.jsp?docid=2000-121508-1457-99.

"Flamer Virus—What Is Flamer Threat | Norton." Symantec Corporation, n.d. Web. 15 Sep. 2013. http://us.norton.com/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east/article.

Harknett, Richard J., John P. Callaghan, and Rudi Kauffman, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," Journal of Homeland Security and Emergency Management 7.1 (2010). Web. 16 Dec. 2013. http://www.homeland1.com/homeland-security-columnists/doug-page/articles/907950-leaving-deterrence-behind-war-fighting-and-national-cyber-security/.

"Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide." *Kaspersky Lab United States*. n.d. Web. 12 Sep. 2013. http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide.

Koh, Harold H. "International Law in Cyberspace" Remarks at USCYBERCOM Inter-Agency Legal Conference, Fort Meade, MD, 2012. Web. 05 Sep. 2013. http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.v.

Koh, Harold H. "Why Do Nations Obey International Law?" *Faculty Scholarship Series Paper 2101*. 1997. Web. 04 Jan. 2014. http://digitalcommons.law.yale.edu/fss_papers/2101.

Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*, 50.3 (2013): 48–53. Web. 24 Sep. 2013.

Lambert, Patrick. "The Basics of Using a Proxy Server for Privacy and Security." *Tech Republic*. ZDNet TechLibrary. 2012. Web. 12 Sep. 2013. http://www.techrepublic.com/blog/it-security/the-basics-of-using-a-proxy-server-for-privacy-and-security/.

Libicki, Martin C. "Brandishing Cyber-attack Capabilities." *Rand.* RAND National Defense Research Institute. 2013. Web. 3 Sep. 2013. http://www.rand.org/pubs/research_reports/RR175.html.

Libicki, Martin C. "Cyber Deterrence and Cyber War." *Rand.* RAND National Defense Research Institute, 2009. Web. 3 Sep. 2013. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Lukasik, Stephen J. "A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for these Domains." *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. 2.3 (2010): 99–122. Web. 10 Aug. 2013. http://www.nap.edu/openbook.php?record_id=12997&page=100.

Lynn, William J. “Defending a New Domain: The Pentagon’s Cyberstrategy.” *Foreign Affairs* (2010): 97–108. Web. 1 Sep. 2013. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Lynn William J. “Remarks on the Department of Defense Cyber Strategy.” *Presentation to National Defense University* 2011. Web. 7 Feb. 2014. http://www.defense.gov/speeches/speech.aspx?speechid=1593.

Mandiant Intelligence Center. “APT1: Exposing One of China’s Cyber Espionage Units.” *Mandian.com*. Mandiant, A FireEye Company. 2013. Web. 15 Sep. 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

“The National Cyber Range: A National Testbed for Critical Security Research.” DARPA. Strategic Technology Office. n.d. Web. 10 Jan. 2014. http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf.

“Onion Router.” *Wikipedia*. Wikimedia Foundation, 03 Feb. 2013. Web. 15 Jul. 2013. http://en.wikipedia.org/wiki/Tor_(anonymity_network).

Orend, Brian, “War”, *The Stanford Encyclopedia of Philosophy* (Fall 2008 Edition), Edward N. Zalta (ed.). 20 Oct. 2013. Web 10 Jan. 2014. http://plato.stanford.edu/archives/fall2008/entries/war/.

Perreault, S. “Common Requirements for Carrier Grade NATs (CGNs).” *Internet Engineering Task Force, Internet-Draft (Work in Progress), Draft-Ietf-Behave-LSN-Requirements-10*. 2012. Web. 10 Jul. 2013. http://www.rfc-editor.org/pipermail/rfc-dist/2013-April/003681.html.

Rattray, Gregory, and Jason Healey. “Categorizing and Understanding Offensive Cyber Capabilities and Their Use.” *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. 2010. Web. 15 Aug. 2013. http://www.nap.edu/openbook.php?record_id=12997&page=77.

Schmitt, Eric and Shanker, Thom. “U.S. Debated Cyberwarfare in Attack Plan over Libya.” *New York Times Online.* New York Times, Oct. 2011. Web. 8 Sep. 2013. http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0.

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

Schmitt, Michael N. “International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.” *Harvard International Law Journal*, Vol. 54, 2012. Web. 18 Sep. 2013. http://www.harvardilj.org/wp-content/uploads/2012/12/HILJ-Online_54_Schmitt.pdf.

Shalal-Esa, Andrea. “Ex-U.S. General Urges Frank Talk on Cyber Weapons.” *Reuters*. 06 Nov. 2011. Web. 07 Feb. 2014. http://www.reuters.com/article/2011/11/06/us-cyber-cartwright-idUSTRE7A514C20111106.

Sheldon, John B. “Deciphering Cyberpower: Strategic Purpose in Peace and War.” *Strategic Studies Quarterly*. 2011. Web. 18 Aug. 2013. http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf.

Smith, David. “How Russia Harnesses Cyberwarfare.” *American Foreign Policy Council*. Vol. 4. Aug. 2012. Web. 15 Jan. 2014. http://www.afpc.org/files/august2012.pdf.

Sterner, Eric, “Stuxnet and the Pentagon’s Cyber Strategy,” n.p. George C. Marshall Institute, Oct. 13, 2010. Web. 10 Sep. 2013. http://www.marshall.org/article.php?id=918.

United Nations. “International Law Commission, Responsibility of States for Internationally Wrongful Acts.” Res. 56/83. Dec. 12, 2001. Web. 05 Aug. 2013. http://untreaty.un.org/ilc/texts/instruments/english/draft%20articles /9_6_2001.pdf.

United Nations Charter. “Signed 26 June 1945, 59 Stat. 1031.”

United States Congress (November 7, 1973). “War Powers Resolution of 1973” (Public Law 93-148).

U.S. Navy,U.S. Marine Corps, and U.S. Coast Guard. “The Commander’s Handbook on the Law of Naval Operations.” Newport, RI: Naval War College. 2007. Web. 15 Dec. 2013. http://www.usnwc.edu/getattachment/a9b8e92d-2c8d-4779-9925-0defea93325c/1-14M_(Jul_2007)_(NWP).

VanRoekel, Steve. “Federal Information Technology Budget Priorities 2014.” *The White House*, n.d. Web. 24 Jan. 2014. www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2014_budget_priorities_20130410.pdf.

Waterman, Shaun. “U.S.-Israeli Cyberattack on Iran Was ‘Act of Force,’ NATO Study Found.” *Washington Times*. 24 Mar. 2013. Web. 12 Jan. 2014. http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all.

White House. HSPD-7, Critical Infrastructure Identification, Prioritization and Protection," Office of Management and Budget. 17 Jun. 2004. Web. 15 Nov. 2013. http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf.

White House. "National Security Strategy 2010." *The White House.* 2010. Web. 22 Jan. 2014. http://www.whitehouse.gov/sites/default/files /rss_viewer/national_security_strategy.pdf.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California