AU/ACSC/2016

UNITED STATES AIR FORCE AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

ACHIEVING CYBER RESILIENCE, REDUCING CYBERCRIME AND INCREASING CYBER DEFENSE CAPABILITIES: WHERE SHOULD THE U.S. DEPARTMENT OF DEFENSE CONCENTRATE TODAY TO PREVENT "CYBERATTACKS OF SIGNIFICANT CONSEQUENCE"?

by

Roby V. Valiaveedu

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Edward Ouellette

Maxwell Air Force Base, Alabama

24 April 2016

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. Government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the U.S. Government.

Table of Contents

Page

List of Figures

Abstract

The purpose of this study is to discover the current state of Internet based cybercrimes and the security threats Information Systems pose at all levels of government and the private and non-profit sectors due to the exponential growth in Internet adoption and usage. This study uses Cloud computing, which is one of the rapidly increasing trends, as an example to emphasize the technological, political, and law enforcement challenges the United States could face in isolating the threat actor. It examines the benefit of the U.S. Department of Defense (DoD) involvement in transnational cooperation and transparency in the form of sharing of vital information used by adversaries. Through a Delphi study that involves subject matter experts from academia, the U.S. Air Force, American nonprofit global policy think tanks such as RAND Corporation and private cybersecurity industry, the study determines whether the Department of Defense's collaboration with the European defense and law enforcement agencies is an effective solution. It will recount the effectiveness of bilateral collaboration within wider partnerships such as the above by the DoD in comparison to the other solutions that will be proposed during the study. Finally, this paper will conclude with its recommendation of the most feasible and effective solution to prevent cybercrimes of significant consequence.

Section 1: Introduction

In the last decade, United States' increasing dependency on the Internet has profoundly changed cyberspace as well as the computing and communication technologies that cyberspace utilizes. Information Technology (IT) powers the U.S. economy, which is approximately a quarter of the world's economy.[1] After an economic analysis and survey conducted in 2013, which includes 7500 private-sector firms and IT professionals in twelve of the world's largest economies, Cisco Systems Inc., concluded that the "Internet of Everything" will create $19 trillion economic impact in net profit globally over the next decade.[2] It is broken down into $14.4 trillion in private sector and $4.6 trillion in public sector.[3] Based on the Boston Consultancy Group (BCG) estimate, in 2016 the Internet-related economic activity is worth $4.2 trillion worldwide.[4] Both cyberspace capabilities and the Internet in conjunction with these technologies enable the free flow of information worldwide and continue to revolutionize how information flows. These increasingly complex, readily accessible and manipulable technological innovations continue to improve the U.S. cyberspace capabilities that empower U.S. society, U.S. businesses, and play an important role in everything U.S. military does, including command and control of forces, intelligence gathering, network-centric operations and logistical support of troops. Furthermore, vast majority of people in many parts of the world are dependent on the Internet as it is one of the key factors in driving Globalization in the 21st century. Today, Internet is the backbone of the global information economy. An open global Internet is vital to ensure that it can continue to empower American enterprises and entrepreneurs. However, cyberattacks attacks are on the rise, bigger, sophisticated, and more damaging than ever before; "the threat from cybercrime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate."[5] In addition to other law enforcement

agencies, cybersecurity efforts are part of the national military strategy as well. In that effort, the United States Department of Defense (DoD) must remain committed and open to engaging with the international law enforcement agencies that are fighting cybercrime on a global scale as it is a global issue demanding a global approach.

At this point, it is important to note the difference between cyberspace, cyberspace capability, and Internet terms mentioned above. Joint Publication (JP) 3-12 defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6] Next, JP 3-12 also defines cyber capability as "a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace."[7] Lastly, National Institute of Standards and Technology (NIST) describe Internet as it is "the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN)."[8]

Due to its position as a world power, its status as the world's largest economy, and its status as one the top ranking innovative economies in the world, the United States is a prime target in cyberspace. The cyberattacks that take place on the United States occur "for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" and lead to cybercrimes, such as information and identity theft. [9] Internet is an element of the information environment in cyberspace. Cyberattack is an illegal, harmful and

hostile activity on the Internet. Terrorists, insurgents, malicious actors and hackers use Internet strategically and tactically, in pursuit of money, power, politics, create fear among targeted populations to keep the propaganda alive, or steal secrets and other sensitive information from trade and weapon secrets to credit card information, cyberattack is often the ways and means to achieve the goal of cybercrime.

Malicious actors exploit the speed, accessibility and inconspicuousness of the Internet and information technologies to conduct cybercrime through a broad range of criminal activities that can occur anywhere throughout the world. Distinguishing between the types of cybercrime enables the identification of the most vulnerable areas that can have significant consequence to the national security. Cybercrime can be categorized into two types: (1) Technology as target: this includes national security offences, distributed denial of services, malware threats, criminal botnet operations, and hacking for criminal purposes as any of these can be used against Americans to instigate fear, intimidation, or public embarrassment or to provide financial support to a terrorist organization. (2) Technology as an instrument: this includes "criminal offences where the Internet and information technologies are instrumental in the commission of a crime, such as those involving fraud, identity theft, intellectual property infringements, money laundering, drug trafficking, human trafficking, organized crime activities, child sexual exploitation or cyber bullying."[10] This research study will focus on the Technology as a target category as the elements of this category are clearly a threat to the "open, interoperable, secure, and reliable cyberspace."[11]

The United States and European Union (EU), which presently consists of 28 countries, are the most vulnerable to cyberattack because their Internet economy is among the largest of the G-20 countries. As a result, the financial institutions in these countries are experimenting with

new technologies to meet the e-business demands such as real-time payments, digital currencies such as Bitcoin, Cryptocurrencies and etc. Hence, targeting these financial institutions is a high-reward area with low risk for criminal hackers. A professional hacker does not take on much risk when committing a cyberattack that impacts the lives of millions. According to Verizon's 2015 Data Breach Investigations Report (DBIR), cyber attackers were able to compromise their target organization within minutes.[12] Cyberattacks include criminal activities conducted via the Internet by a wide diversity of cyber-threat actors such as criminals motivated by greed; foreign governments and/or their supported groups such as the patriotic hackers; non-state actors; and hacktivists promoting a political agenda or antigovernment activists. Criminal actors' activities include the following: cyber espionage; online scams and phishing activities; confiscating online bank or credit card accounts; obtaining and exploiting personally identifiable information (PII) for stealing money from victims' financial accounts or selling PII for others to do the stealing; creating and distributing viruses to infect the victims; posting confidential, personal, business or government information on the Internet; disrupting country's critical national infrastructure; and cyber-sabotaging by contaminating hardware or software through Internet causing disruption or destruction of manufacturing processes, damage of equipment or information. Therefore, a threat actor can use the Internet as a double-edged sword. For example, cyber terrorists can use the Internet to steal, generate and transfer needed funds to support their political or ideological objectives and also use it against their enemy for deception or cause destruction through large-scale cyber weapons such as viruses or botnets. For example, the anti-Islamic State hacker group GhostSec recently located $3 million of the hard-to-trace bitcoin owned by an Islamic State of Iraq and the Levant (ISIL) member.[13] DDoS attacks by some well-known Islamic groups on 19 thousand governments and private French websites after the January 7, 2015 Charlie Hebdo

Massacre as well as the hacking of U.S. Central Command's (CENTCOM) twitter and YouTube accounts around the same time by the ISIL's "Cyber Caliphate" are two of the most recent examples to highlight how successfully an enemy can react to world events.[14, 15]

The new area of Cloud or "the Internet" computing is playing a major role in transforming the economics of information technology and also a new role in cybercrime. Cloud computing is an Internet based information technology infrastructure, in which on-demand computing resources-- such as servers, storage and applications --themselves are distributed throughout the Internet. Therefore, Cloud can be accessed anywhere in the world through any Internet connection. Regardless of the business size, it allows organizations in all sectors to expand network capacity, increase operational output and improve organizational agility, optimize costs, and meet compliance mandates quickly and efficiently at a small fraction of the cost of owning and maintaining legacy servers, storage systems, software licenses, facilities and etc. Global Industry Analysts, Inc. (GIA) estimated that the Cloud computing saves companies more than 35 percentage of potential information technology related costs.[16] Cloud services are on strong incremental growth. According to Gartner analysts, the estimated global market for the public Cloud services will reach $204 billion in 2016, which is a 16.5 percent increase over the 2015 market, $175 billion.[17] 2015 reports show that that 87 percent of organizations are making use of Cloud infrastructure.[18] Over all, Cloud computing system is becoming a transnational public utility that provides progressive computing power for startup businesses to large enterprises. It will continue play a vital role in the growth of the global economy.

With the many advantages that allow enterprises to gain huge financial returns from Cloud computing while getting the most out of their Cloud based IT infrastructure, Cloud computing comes with many security drawbacks that are mostly same as on-premises IT

deployments. However, Cloud offers many unique choices for attackers. For example, hackers can obtain large amount of data in less time as highly efficient Cloud platforms are networked on high bandwidth. In addition, a hacker may create a virtual machine (VM) to conduct malicious activity that can go undetected due to the vulnerability of the Cloud. After the use, the hacker can terminate the VM, which removes the critical digital footprints that are valuable for the forensic investigation. In many cases, attack data may be located in different jurisdictions with which the victim state has no treaties signed for cooperation. Lastly, malicious actors can use the supercomputer-quality processing power from the Cloud to develop new and strong types of malware. In a survey of 100 information and communication technology (ICT) professionals at the 2010 hacker conference, 96 percent believed "Cloud would open up more hacking opportunities for them" and 45% stated that they had "already tried to exploit vulnerabilities in the Cloud."[19]

Cybercrime is a transnational crime. However, "some experts believe that establishing a comprehensive, binding cybercrime convention may be impossible given fundamental differences in opinions between countries about the Internet."[20] Given the complexities of cross-border use of Cloud services and uncertainties surrounding cyber activities, extensive and integrated transnational cooperation is enormously important. All of the world's population who has access to the Internet relies on the same Internet infrastructure. The Internet exists in every country in the world and is relatively open in most countries. In this way, cyberspace has no jurisdictional boundaries. Therefore, "country-specific mandates will not address the threat because it is a quintessential transnational threat that requires global cooperation."[21] This proper transnational cooperation should ensure the rapid flow of information and evidence while windows of opportunity are still open to identify the perpetrator. In addition, this transnational

cooperation should involve transparency in the form of information sharing and dialogue. This transnational cooperation is a necessity to progress an effective counter measurement against the challenges posed by cybercrimes within and outside the U.S. One of the best examples of the transnational cooperation that exists today is the strategic and the operational level cooperation between the member States of the Council of Europe (CoE) Convention on Cybercrime (the Convention), often referred to as the Budapest Convention.

Economic cybercrime surveys and research data agrees that the overall Internet penetration has steadily increased in the last six years in our tech-dependent and interconnected world.[22] Today's changing technological advances due to the global populations' demands bring about new ways to interact with one another. Cybercrime poses serious logistical challenges that prevent tracking and apprehending a talented cybercriminal as well as preventing a cyberattack. As more enterprises and organizations are utilizing Cloud computing service models as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) for cost saving and infrastructure independence, it creates a cyberspace safe haven for the diversity of cybercrimes including cyberterrorism, cyber espionage, cyber sabotage, and terrorism financing. In fact, businesses using Cloud environments are widely seen by hackers as "a fruit-bearing jackpot" as they would prefer safety and greater return by investing little time to conduct their criminal activity.[23] In recent years, the use of the Cloud in its anonymous, scalable and borderless nature has created in cyberspace a fertile ground for new and innovative cybercrimes.

As technology is evolving into Cloud computing, cybercrime investigation and cyber forensics are also evolving because of their direct correlation to the evolving technology. However, unlike technology, these criminal investigative sciences are affected by organizational,

societal and legal challenges that require international collaboration. Malicious individuals can perform attacks from virtual machines inside the Cloud and then terminate the machine or compromise the data under investigation with malware after the intended purpose and leave no trace of the attack. That emptied space possibly could get overwritten in Cloud quickly; leaving very little data for the investigator. Likewise, since investigators cannot access the virtualized environment in a public Cloud system physically, forensic examinations of cybercrimes occurring in the Cloud are different by far in comparison to an attack on a local private network. In addition, data acquisition procedures' challenges possibly involve multi-jurisdiction and multi-tenancy as well as legal regulations and agreements. Therefore, local and national agencies operating in isolation are certainly not making the best use of their resources.

Research Question

The United States Department of Defense is continually seeking to strengthen its cyber defense and cyber deterrence posture to defend DoD networks, systems, and information, defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence, and provide cyber support to military operational and contingency plans. It is worthwhile to improve the efficacy of DoD's digital forensic investigations in deterring and responding to online threats. This question is not suggesting DoD go after the small number of top-tier cybercrime actors and the criminals out to make money, but it does suggest an effective solution to prevent, deter or detect terrorists and state-sponsored hackers who are capable of initiating a catastrophic cyberattack. This solution should also support the U.S. counterinsurgency campaigns to identify those groups hiding money-mining botnets in the Cloud to fund their ideology campaigns as well as those who are attempting to instigate fear, intimidation, or public embarrassment to the U.S. societies and its government.[24] Due to the unchartered risks and

challenges associated with Cloud computing, it is important to overcome challenges associated with digital forensics when isolating malevolent actors

Non-state actors such as ISIL, Al-Qaida and Hezbollah or antigovernment activists do not need sophisticated weapons similar to the Stuxnet worm. At this point, these non-state actors can still use resilient and low-cost botnet malware for covert intelligence collection, or as weapons of their ideology campaigns. For example, a botnet can be used to launch coordinated attacks such as distributed denial of service (DDoS) attacks against any of the sixteen critical infrastructure sectors that the people of the United States are heavily depended on for their day-to-day needs in homeland or elsewhere in the world where the U.S. has security interests. Therefore, international collaboration to create and innovate against cybercrime, especially cooperation with all the Convention member States in the area of legal challenges is vital. In addition, working with partner organizations to achieve a successful cyber forensic intelligence using the existing treaty supporting consensus-based international standards are vital to solve the future complex and dynamic challenges Cloud computing introduces as it become widely used.

Methodology:

This research will use a mixed methods approach in which information is collected both quantitatively through the comparison of cybercrime data presented in 2013, 2014 and 2015 cyber threat reports from various sources and qualitatively through a modified Delphi study. This research project occurs in two parts and has an exploratory sequential mixed methods design. The mixed method approach is utilized so the quantitative data can validate the questions used in the first questionnaire of the Delphi technique. The Delphi technique was chosen because researching an effective solution in the area of cybercrime prevention or effective cyberspace deterrence in an increasingly complex landscape of rapidly changing

technology is multifaceted and dynamic. The Delphi method allows for a structured group communication process that provides a consensus from a group of experts in the field.

This research project occurs in two parts. In part one, the quantitative data from the three threat reports prepared by Internet security companies in the United States and the United Kingdom, (one of the EU member States), as well as Europol will be reviewed for the "technology as target" cybercrime category. The quantitative data will be analyzed to identify the most vulnerable area where transnational government and enterprises collaborate to conduct successful investigation and identify flows in the transnational cybersecurity measures as well as the core capabilities necessary for preparedness, prevention, and deterrence against cybercrime. The conclusions drawn from part one will also provide insight into the development of a questionnaire that will be used in part two, the Delphi technique portion of the research study.

The Delphi technique was chosen to find an effective and practical solution for a global problem that has far-reaching effects. Delphi is a method for the "systematic solicitation and collation of judgments on a particular topic through a set of carefully designed sequential questionnaires interspersed with summarized information and feedback of opinions derived from earlier responses."[25] In phase one, a question will be presented to the panel of experts. This serves to generate ideas that will be used to find solutions for a stronger deterrent posture against cyberattacks. The data from the first questionnaire will be analyzed and responses to the questions will be categorized by frequency. In phase two, re-evaluating panel members answer questions from phase one in light of other participants' response. The data from the second questionnaire will be analyzed and the process will be repeated once again in phase three to obtain a consensus.

Limitations of the Study

The present study has several limitations. Firstly, finding the solution to the research question is based on a small number of Delphi study panelists. Secondly, this study relied only on publically available information and lacks a comprehensive overview of all forms of information including those that are confidential and internal within the DoD such as the information pertaining to DoD's latest cyber defense capabilities, and cyber threat data. Thirdly, the cyber capability is accelerating at an increasingly rapid ppace, especially the growing landscape of cyber technology integration, cyber defense and cybersecurity that any sources publications regarding cyber forensics becomes obsolete very quickly. In order to compensate for this limitation, this study heavily relies on reputable news sources, government organization's websites, most recent cyber threat reports prepared by private industries, and cybersecurity studies conducted in recent years in addition to the books, government publications and scholarly journals. Still, however, the information received from these news sources may be incomplete. Finally, due to the constricted timeframe in which the research was conducted, this study could not fully assess the effectiveness of transnational cooperation in achieving cybersecurity.

Question Background and Significance

According to United States Government Accountability Office (GAO), an official from one of the key U.S.-based software companies stated that in order to resolve a major cybersecurity breach that occurred in 2009, it had to work with each of the 28 member States of the European Union (EU) individually.[26] The increasing world-wide interconnection of computer networks, in conjunction with increased sophistication of cyberattacks over time, validate the need for a better understanding of how to prevent and respond to cybersecurity emergencies. Studies indicate that the United States and the European Union will remain a key target for

cybercrime, particularly because of their economies' Internet-dependency in the areas of business, government and military.[27] These studies also highlight that in 2014, 205 days was the median number of days attackers were present on a victim network before they were discovered; such length is unacceptable for free market economies.[28] For quick and effective cyber counter-terrorism and cybercrime measures, valuable information can be shared with the working-group states through the legal frameworks consistent with the Convention. This joint effort enables the ability to detect severe malicious cyber-enabled activities rapidly and permits forensics experts to recover evidence during the valuable window of opportunity for identifying the perpetrator. In addition, it helps the DoD to secure additional intelligence about the adversaries' cyber capabilities in real-time. Therefore, it is important to evaluate the current state of cyber space and demonstrate the need of a joint multinational approach to ensure "robust incident management, resiliency, and recovery capabilities for information infrastructure."[29]

In a research study by National Academy of Sciences, Mr. Sofaer indicated that the United States is especially vulnerable to cyberattacks because it depends on cyber systems more heavily than most other states. He goes on to explain, there is a great range of differences of cyber activity among international states and cyber systems. However, international agreements can still prove to be valuable. The cyber activities that are appropriate for international agreements must be identified. Tools needed to increase cybersecurity in different areas of activity are appropriate for international cooperation.[30] Current research indicates that transnational cyberspace standards will increase stability and predictability of state behavior in cyberspace, and these standards will enable international actors to take required countermeasures.[31] However, current research lacks the explanation regarding the feasibility of the U.S. Department of Defense collaborating with international counterparts through sharing

information that is critical to understanding its adversaries, specifically the state-sponsored cybercrime actors and cyberterrorism actors. Existing literature emphasizes "the ease with which the origins of cyberattacks can be hidden, and the fact that cyberattacks on one nation can come from anywhere on the globe, means that cybercrime and cyberterrorism are truly international threats."[32]

Section 2: State of the Cybersecurity in the United States – Brief Overview

The United States makes up the third largest geographical demographics of Internet users; consisting of 276.6 million users.[33] A vast majority of people who live in the United States have bank accounts and associated credit or debit cards, which they use for products and services available through online. The 2012 through 2015 cybercrime surveys show it was among the countries most targeted globally by sophisticated cyberattacks. Moreover, the U.S. cybercrime survey found that the overall cybercrime incidents and associated financial losses are on the rise.[34] Consolidated incidents data from 70 different organizations in 61 countries illustrate that there were 79,790 security incidents including 2,122 confirmed data breaches in 2014.[35] Despite the fact that achieving cyber resilience is one of the U.S. strategic priorities and the U.S. government has issued various directives and initiatives, data shows that in 2014 just over two-thirds, or 72 percent of incidents globally, occurred in the United States, with 1,107 breaches.[36] The second-largest percentage of breaches was among the EU, with 175 or approximately 11 percent of the breaches.[37] Additionally, based on a study sample of 58 organizations in the United States alone, 2015 data showed an increase of 19 percent in comparison to 2014 cybercrime data, and an 82 percent increase in comparison to 2009 cybercrime cost.[38] At the present time, Eastern Asia, Eastern Europe, and Latin America, where the most cybercrime actors are located, leads in the number of cybercrimes being committed, and

Russia leads in the quality of cybercrimes being committed.[39] The rising number of security breaches in United States, despite the best practices and measures organizations are taking, speaks to the fact that there is no guarantee against being breached. It can also affect the general public's negative perception of their government's realistic strategy to secure cyberspace.

Data Breaches in the United States

All information technology security surveys conducted in previous years show that cybercrime is on the rise and the cybercriminals continue to outwit deterrence and detection. Most data breaches in 2014 were carried out through hacking. Data breaches are now a part of American life. American government, financial, education and retail services, healthcare, communications, technology, consulting and transportation industries have suffered significantly from data security incidents. Ponemon Institute research surveys conducted in 2013 and 2014 show that 110 million or 47 percent of adults in America are victims of cybercrime.[40] It estimated that 442 million online accounts associated with Americans had been compromised during the same timeframe. Further, cybercrime is the leading cause of the medical data breaches that involves millions of patients annually.[41] CSIS estimated that the United States lost about $100 billion in 2014 due to cybercrime. It includes the loss of intellectual property and business intelligence, as well as the costs to companies for recovery and defense. In the United States alone the average loss due to cybercrime cost a U.S. company on average $15.42 million in 2015, while the global average was $7.7 million.[42] In his 2015 *National Security Strategy,* the President recognizes "the danger of disruptive and even destructive cyberattack is growing, and the risk of another global economic slowdown remains."[43] Private and public organizations in the United States continue to address cybersecurity issues as an add-on IT component to protect themselves from litigation and adverse publicity. However, just adding more of the same

available technology will not be a risk-free solution against cyberattacks, but only increases the severity and sophistication the cyber threat. An effective counter cyberattack measurement has to be developed at the international level to identify emerging cyber threats at their inception, and sharing intelligence will enable the victim country or the partner nation to take necessary measures to counter them.

Security and Capacity to Defend

Achieving cyber resilience, reducing cybercrime and increasing cyber defense capabilities are three of the top objectives in both the U.S. and EU's cybersecurity strategy. Cyber resilience is the ability to recover and resume systems operations in the face of persistent adversity. It incorporates best practices and standards for cybersecurity and improves detection and prevention or recovery from previously unknown malicious activity or attacks. Cyber resilience enables Information Systems that rely on cyber infrastructure to continue to provide services while remaining resilient against cyberattacks.

Decreasing cybercrime involves identifying risks and implementing the National Institute of Standards and Technology's (NIST) Cybersecurity framework in order to reduce exploitable weaknesses and attacks. Further, remediation of vulnerabilities through deploying and upgrading software, and deploying innovative and more secure protocol and routing technology are also significant. When an organization forgoes or postpones "leading practices from various standards bodies that have proved to be successful when implemented," it is promoting cybercrime and putting the fundamental freedom and privacy at risk.[44] Reducing cybercrime also involves expanding transnational cooperation to increase collective security by leveraging capabilities, reducing collective risk, fostering multi-stakeholder initiatives, and adapting to internationally common cybercrime laws that enable evidence-sharing, extradition, and other

types of coordination.[45] There is no foolproof formula to prevent cybercrime nor can a single-nation fix cybercrime issues on its own.

Together with land, sea, air and space, cyberspace is the fifth operational domain of security. The cyber domain represents vulnerability and opportunity. "The speed of cyberattacks and the anonymity of cyberspace greatly favors the offense."[46] The cyber defense involves both taking the advantage of that opportunity and capitalizing on information dominance while addressing that vulnerability.[47] It also involves implementing surveillance programs for better cyber defenses against malefactors who are the most prevalent threat on the Internet. These programs reduce the risk of cyberattacks against infrastructure, financial institutions, commercial enterprises and citizens. DoD's open source sharing of innovative technologies can be seen as an effort to increase cyber defenses. For example, NSA released the source code for "Niagarafiles (NiFi)" data management software that promotes data network interoperability and effective transmission of critical data without artificial delays. This particular Open Source Software (OSS) tool can be perceived as a platform that can manage, analyze, and handle large data flows simultaneously for better cyber defense. A widely-used Open Source Software that is managed at a popular and trusted repository, such as the Apache Maven, is highly secure and cannot be compromised by just being open source code. Open Source Software that is well-known and extensively used often has very little security risk. Its source code is public; thus, experts, the end users, and the community of open-source software projects at large verifies whether it is secure or has backdoors for surveillance and other malicious activities. Unlike proprietary commercial software, an OSS such as Apache NiFi is exposed to thousands of engineers worldwide who are interested in its integration. When they find vulnerabilities, they report their findings, quickly patch and incorporate code changes for the

distribution. Only approved trusted software developers or engineers can modify the trusted repository directly (see Figure 2.2.1 in Appendix E).[48] The U.S. Department of Defense uses hundreds of OSS programs today.[49] They include both the military-specific and commercial OSS programs.

While cybersecurity risk management alone cannot stop the cyber threat as the severity and sophistication of the cyber threat continues to rise, cyber defense involves pursuing partnerships with businesses that make up the nation's critical infrastructures in all sectors to obtain data breach reports as quickly as possible. President Barack Obama's *International Strategy for Cyberspace* states that "the future of an open, interoperable, secure and reliable cyberspace depends on nations recognizing and safeguarding that which should endure, while confronting those who would destabilize or undermine our increasingly networked world."[50] Further, DoD's Quadrennial Defense Review 2010 highlights the following four steps to strengthen its cyber defense capabilities: (1) develop a comprehensive approach to DoD operations in cyberspace; (2) develop greater cyberspace expertise and awareness; (3) centralize command of cyberspace operations; and (4) enhance partnerships with other agencies and governments.[51] Cyber defense is the prevention or disruption and neutralization of cyberattacks from both criminal and state-sponsored adversaries as they happen in real-time. Capabilities to discover, define, analyze and mitigate cyber threats and vulnerabilities are vital to defend the U.S. homeland assets and protect U.S. interests. While all these capabilities are important, without the crucial transnational cooperation that is a long way away, it will be difficult for nations to combat cybercrime, cyberterrorism and cyberwarfare.

Cybersecurity Capabilities in the United States

The Department of Homeland Security (DHS), a civilian agency, plays a vital and leading role in strengthening the U.S. cybersecurity preparedness and cyber resilience, which is a U.S. strategic priority. In 2010, DHS and DoD agreed on building a new framework to improve operational coordination and joint program planning. This joint force effort formalized processes in which DHS and DoD work together to protect the U.S. "cyber networks and critical infrastructure, and increases the clarity and focus" of both agencies' respective roles and responsibilities.[52] This jointness made it possible for DHS to effectively leverage vital technologies, personnel, and a tremendous amount of cyber expertise at the National Security Agency/Central Security Service (NSA/CSS).[53] Further, the DHS and DoD interoperability also permits NSA and other DoD agencies to effectively support civilian authorities during the cyberattacks on the homeland. [54] The National Cybersecurity and Communications Integration Center (NCCIC) is the DHS' main processing center and the United States' unified operations center for threat information sharing and response. Several organizations such as DHS components (ICE, USSS), DoD, intelligence community organizations, State governments, law enforcement, private sector and non-governmental partners are integrated into the NCCIC (see Figure 2.2.1.1 and Figure 2.2.1.2 in Appendix E for the Organizational Chart). This consolidation of a number of communications operations centers strengthens the United States' ability to manage significant cyber incidents. It is a "24x7 operations center that provides both situational awareness and analysis, and significant cyber incident response capabilities."[55]

One of the most effective tools the DHS uses today is the National Cybersecurity Protection System (NCPS), which is three versions of EINSTEIN: EINSTEIN 1/Network Flow; EINSTEIN 2/Intrusion Detection; EINSTEIN 3 A/Accelerated Intrusion Prevention. EINSTEIN

is “a suite of technologies intended to detect and prevent malicious network traffic from entering and exiting federal civilian government networks.”[56] However, according to GAO, the $1.2 billion program to-date has weaknesses in in the limited capabilities in detecting and preventing intrusion. These limitations include: 1) Its use of “only one of three detection methodologies identified by NIST: signature-based, anomaly-based, and stateful protocol analysis;”[57] 2) The capabilities that are currently in use only prevents “a limited subset of network traffic.”[58] In the effort to increase national cyber resilience, DHS prioritizes securing federal government’s nonmilitary networks, protecting critical infrastructure and responding to cyber threats.

Although the DHS has the lead role in cyber resilience and in reducing cybercrime, by executive order, “NSA acts as the national manager for National Security.” [59] NSA plays a prominent role in developing and deploying high-tech cyber defense tools. Further, the U.S. Cyber Command (USCYBERCOM), a sub-unified combatant command subordinate to the Strategic Command (USSTRATCOM), retains responsibility for defending U.S. military networks, improving “DoD’s capabilities to operate resilient, reliable information and communication networks, counter cyberspace threats, assure access to cyberspace,” providing offensive cybersecurity capabilities, including cyber warfare.[60] An overwhelming number of potential vulnerabilities to cyberattacks exist in the military networks as the DoD currently operates in 88 different countries involving more than 15,000 different computer networks across 4,000 military installations.[61] The USCYBERCOM “unifies the direction of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD’s cyber expertise.”[62]

USCYBERCOM is comprised of cyber units associated with all five branches of the U.S. Armed Forces. It includes Army Cyber Command (ARCYBER), Air Force Cyber Command

(AFCYBER\24th Air Force), Fleet Cyber Command (FLTCYBER), Marine Forces Cyber Command (MARFORCYBER) and Coast Guard Cyber Command (CGCYBER). All of these five service elements are also subordinate to DHS as well. USCYBERCOM is capable to conduct full-spectrum military operations. Its mission is to ensure the United States freedom of action in cyberspace and to deny the adversaries the same.

According to the Bills and Statutes of the United States, Title 18 U.S.C. Section 1030, if a cyberattack is a threat to national security, and the Federal Bureau of Investigation (FBI), under Department of Justice (DoJ), is the lead investigating agency. Otherwise, FBI and the United States Secret Service (USSS), one of the agencies under DHS, have the authority to investigate all criminally motivated cybercrimes.[63] However, after receiving reports on any instances of cyberattack, agencies analyze large amount of digital forensic data to identify whether the cyber-attack incident was a criminally motivated or was a national security threat. Therefore, a lack of one unified and dedicated Cyber Crimes Center can be confusing to the private sector when reporting a cybercrime or sharing the critical data for the forensic research during the time sensitive investigation. This confusion delays the process to trace the physical source of an attack during a limited, important window of opportunity for attribution. Besides USSS, DHS also has Immigration and Customs Enforcement (ICE) – Cyber Crimes Center (C3), which maintains close working relationship with the USSS and the European Cyber Crimes Center (EC3). Overall, the United States does not have a designated cybercrime investigation agency. In its place, several federal law enforcement agencies those under DHS, DoJ, and in some cases DoD are involved.

Internationalization of Cybersecurity

There is no such a thing as perfect cybersecurity.[64] "No one can predict every new intrusion technique."[65] Collaboration between the United States Department of Defense and Europol's EC3, which helps protect 28 EU member States' citizens and businesses against cybercrime threats, would be the most effective in improving cyber forensic technologies to prevent or disrupt cybercrimes. This collaboration can leverage the essence of international cybercrime treaty, the Convention. Preventing cybercrime requires mutually beneficial partnerships among foreign government agencies. Through these partnerships, foreign government agencies can share information in a timely manner, assist each other through the already established Convention to investigate cybercrimes and provide an efficient and well-timed solution that is founded on global tenets. This form of joint, interagency, intergovernmental, and multinational strategic and operational approach is necessary for partners in integrating intelligence and developing adequate forensic cyber technologies that can isolate the source of threat, and deter malicious actors. Collective and individual security can be achieved through efficient coordination between partner nations including their private or corporate businesses. For quick and effective cyber counterterrorism measures valuable information can be shared with the working-group states, requiring the examination of multi terabytes to petabytes of data (in Cloud) on a routine basis.

Section 3: The Council of Europe Convention on Cybercrime

The first international, and most significant, multilateral treaty to prevent cybercrime was the Convention on Cybercrime entered into force in 2004 that has been ratified by 48 countries, as of 10 March 2015.[66] It is the only legal mechanism designed to facilitate collective transnational cooperation to fight cybercrime. For any member States, it is a tool to advance

common objectives in the area of cyber security, either bilaterally or multilaterally with the other 47 member States. It addresses several categories of computer-related crimes: fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability. The efforts on the Convention began in 1997 to establish an internationally recognized common criminal policy that involves rapid and effective international cooperation in monitoring, detecting, investigating, collecting electronic evidence and prosecuting any cyber-criminal offense to tackle computer-related crimes and end cybercriminals' "feeling of impunity" from the pursuit by domestic or international law enforcement. The Council determined that cybercrimes, including hacking, and attacks or spread of destructive computer viruses, can only be tackled at the global level because of the transnational nature of the cyberspace. September 11, 2001's unprecedented terrorist attacks fast-tracked the efforts to first ratify this multilateral treaty. The treaty planners identified urgent security problems such as the threat of cyberattacks on critical infrastructure facilities, financial institutions, or government systems, as well as terror organizations' use of cyberspace to communicate, spread propaganda, raise money, and recruit.

Benefit and Reliability of Treaty

Several U.S. Congressional measures on cybercrime, cyberterrorism and cybersecurity such as the USA PATRIOT Act of 2001, and the Homeland Security Act also are stipulated in the Convention.[67] A multilateral-level U.S. cooperation with the member States of the Convention on the Cybercrime is important especially when some of the European countries such as Belgium, France, Germany, the United Kingdom, and the Netherlands are at risk of terrorist attacks as radicalization and jihadist violence are on the rise in these countries.[68] For a quick and effective cyber counter-threat, valuable information can be shared with the working-

group states allowing the forensics experts to recover evidence during important windows of opportunity for attribution. In addition, it helps the U.S. to secure the best possible intelligence about potential adversaries' cyber capabilities. Without such collaboration and with the cyber technology shift into Cloud computing, the DoD will miss the opportunity to innovate against massive cyberattacks in a timely manner, challenging the threats and helping to secure cyberspace for American society and the global community. When it comes to international collaboration to address cybercrime and conduct a successful investigation, the Convention includes all the elements that are necessary to assist the member States' cybercrime investigation and prosecution of the culprit(s). At the same time, the Convention promotes cyberspace as an area of fundamental rights, freedom of expression, global connectivity and access to information.

Issues and Concerns of Treaty

The American Civil Liberties Union (ACLU) raised concerns on the lack of balance of law enforcement's viewpoint and the U.S. constitutional viewpoint, especially in the area of privacy and civil liberties limits. The treaty drafting committee consisted mostly of law enforcement. Additionally, the industry and public interest groups' perspectives were absent when drafting the treaty.[69] Four of the world's top emerging economies, often referred to as the BRIC nations (Brazil, Russia, India, and China), who have a history of proposing Internet rules, claim that the Convention is inherently inapplicable to non-European countries. Brazil, China and India argue that it is a treaty that is negotiated by Europe and the United Sates "despite the fact that non-European countries are party to the convention and those whole swaths of international law—still valid today—stem from negotiations amongst Europeans." [70] Furthermore, Russia and China argue that the Convention violates state sovereignty, a claim that has been discredited by the Cybercrime Convention Committee.[71] Lastly, some critics argue that

the Convention is not prepared by the UN, but by the Council of Europe and it is a "convention of the victim countries" which lacks some of the important countries with the highest cybercrime rates in the world, such as BRIC nations. Therefore, the Convention is limited in its efficacy of efforts to improve international cooperation.[72] Three of the BRIC nations, Brazil, Russia, and China are among the top five cybercrime hotspots in the world.[73] Although all nations agree on the importance of transnational cooperation to "tackle a crime that knew no boundaries;" some spoke of a need to launch a brand new global cybercrime treaty "under United Nations auspices, and to address regional concerns on cybercrime."[74]

Section 4: Problem Description

Today, more than 3.3 billion of the world's population uses the Internet. It continues to grow rapidly with a growth rate of 832 percent since 2000, from 738 million Internet users. That is an increase from seven percent of the world's population to 46.4 percent in 15 years.[75, 76] During this timeframe, mobile technology utilizing cyberspace has evolved as well as Internet speed- bandwidth.

The notion of the Internet of Things (IoT) took its root and enabled an exchange of data never before available. Cisco Systems, Inc. estimates the IoT will consist of 50 billion devices connected to the Internet by the year 2020.[77] This kind of powerful and fundamental cyber technological shifts will continue to take its part in shaping the global economy in our interconnected world. With such shifts, nations will have to find more effective and efficient ways of fighting cybercrimes, cyber espionage and cyber sabotage. Since new technologies such as Cloud computing have opened the door to many new forms of cybercrimes that have the potential to give an advantage to the attacker in continuing and increasing their criminal

activities in cyberspace, the need for new ways of fighting cybercrime has become even more urgent.

The Global Economic Crime Survey 2016 ranks cybercrime as one of the top two economic crimes in the world, and it has been on a steady increase to become the top economic crime.[78] A comprehensive study conducted in 2014 by the Center for Strategic and International Studies (CSIS) has found that the "annual cost to the global economy from cybercrime is more than $445 billion, including both the gains to criminals and the costs to companies for recovery and defense."[79] The lack of cutting-edge cyber forensics tools as the technology itself is rapidly changing, and the challenges law enforcement faces in the international arena due to the legal challenges, created cybercrime a growing industry. Concentrating the effects, offensive actions, surprise forces and sustainment of security are dependent on the quality of intelligence both in the cyber world and the physical world. As world's entire population shares cyberspace without a predefined physical boundary, maliciously altering the technology that creates the virtual boundaries allows anyone to virtually infiltrate inside the security boundaries set by others. Therefore, sustainability of cyberspace standards will be based on the Convention member States' increased openness in providing law enforcement cooperation including information and evidence, interoperability, and reliability of the commitments they set.

The President's 2015 *National Security Strategy* states that the U.S. is shaping "global standards for cybersecurity and building international capacity to disrupt and investigate cyber threats."[80] The Convention's aim is just that, and since the United States is one of the member States of the convention, such partnerships can increase resilience, predictability of cyberattacks, information security including protection of privacy, and openness and stability of the Internet in

the cyber domain. It may also allow the DoD to take any required counteractive processes while windows of opportunity to isolate the malicious actor are still open.

Problems in the Near Future

One of the future challenges is the development of tools for forensics investigators to uncover, gather, examine and interpret digital evidence to help solve crimes. To be efficient and effective, these forensic investigation tools can only be developed through the international cooperation. [81] These tools enable forensics that work along with the non-localized nature of Cloud computing environment that can physically exist on a foreign server. The National Institute of Standards and Technology (NIST) has identified sixty five technical challenges that Cloud computing poses to forensics investigators in nine categories ranging from architecture (such as diversity, complexity, provenance, multi-tenancy and data segregation), data collection (such as data integrity, data recovery, data location and imaging), analysis (such as correlation, reconstruction, time synchronization, logs, metadata and timelines), standards (such as standard operating procedures, interoperability, testing and validation), training (such as forensic investigators, Cloud providers, qualification and certification), anti-forensics (such as obfuscation, data hiding and malware), incident first responders (such as trustworthiness of Cloud providers, response time and reconstruction), legal (jurisdictions, laws, service level agreements, contracts, subpoenas, international cooperation, privacy and ethics) to role management (such as data owners, identity management, users and access control).[82] The traditional evidence-gathering for forensics work and legal jurisdiction in obtaining evidence is not applicable to the Cloud computing environment as "the laws vary on the legal protections regarding data in the Cloud from country to country."[83] Therefore, if forensic investigators seize

a mobile device or a computer at the crime scene that is linked to pooled resources in the Cloud, they will not be able find corroborating evidence.

Section 5: Delphi Study

A Delphi study was conducted to find effective and practical solutions to the problem of increased sophistication and frequency of cyberattacks against U.S. organizations. Leveraging the three phases of this study, it will identify the best approach for effective protection against all cybersecurity threats. Literature reviews and quantitative data analysis of several cyber threat reports revealed that the Cloud computing introduces significant new avenues of attack. To find solutions for effective combating, prevention, deterrence and detection of potential cyberattacks, the following question was posed to five panelists: "What could help the U.S. Department of Defense (DoD) prevent cybercrimes of significant consequence, especially with the rapid increase of Cloud computing?" The majority of sources used for this study underscore the current state of cybercrime, and call for transnational cooperation with transparency in the form of information sharing and dialogue. One solution was provided to the panelist to either agree with, or provide one of their own. The solution that was provided to the panelists proposed DoD's collaboration with a key agency that is helping to combat the global scale and scope of cybercrimes, Europol's EC3. The Europol's European Cybercrime Centre was chosen because it collaborates with 28 EU Member States where several of those States are potential targets of cybercrime. It also partners with many non-EU law enforcement agencies, international organizations, academia and numerous companies involved in Internet security and the financial sector. Additionally, most of the EU Member States ratified the Convention on Cybercrime. The Convention on Cybercrime is an important element for the transparency in the joint effort to make the best use of these nations' resources dedicated to combat cybercrime.

Three rounds of the Delphi took place. Each round was distributed by email. The selected panelists were subject matter experts from academia, the U.S. Air Force, global policy think tanks and private cybersecurity industry. The participants were kept anonymous from each other throughout the process. Their participation entailed the following three phases: (1) brainstorming- for the question presented above, the panelists were asked to provide solution statements and their rationale that can be achievable in a short period of time in comparison to the proposals such as "UN Cybercrime Treaty," which could take a decade or more of negotiations; (2) evaluation- the panelists were asked to re-evaluate their response in light of other participants' responses and pick the top most feasible and effective solution and a (top) alternative solution from the consolidated list of "phase one;" and (3) consensus- each panelist responded to a final email to obtain a consensus on the best proposed solution that will help DoD to effectively and efficiently prevent cybercrimes of significant consequence. Further information on the process of this study has been provided in Appendix A through Appendix D.

Delphi Study – Round 1 Through Round 3

The first round of the Delphi study called for subjective intuitive farsightedness from the subject matter experts on the most desirable and feasible solution for reducing cybercrime and increasing cyber defense. The core of the problem was the current increased sophistication and frequency of cyberattacks against U.S. organizations. Given the fact that the technological basis, logistics, tools, and operational ways and means of cyber activity such as cybercrime, cyberterrorism and cyberwarfare are all common to each other, the panelists provided several solutions and supporting rationales to the given problem.

Initially, the two solutions emphasized the need for a wider transnational cooperation in which the U.S. Department of Defense collaborated with other nations' defense or law

enforcement agencies combating against cybercrime such as the European Defense Agency (EDA) and Europol's EC3. Panelists who suggested these solutions endorsed leveraging the Cloud to facilitate collaboration between the partner nations in sharing Tactics, Techniques and Procedures (TTPs) used by adversaries. They believed such cooperation not only ensures the rapid flow of information and evidence that can effectively trace the physical source of an attack on a near real-time basis, but also would give the opportunity for DoD to develop advanced digital forensic tools. This cooperation at the multilateral level will provide a unique opportunity for attribution. It is a win-win proposition as it ultimately benefits all parties involved.

Next, another solution to the problem suggested by a panelist was that the DoD can reduce the incidents of cybercrime by resourcing the requirements of a cyber deterrence policy.[84] The rationale was that there are several countries (e.g., Russia), that protect their cybercriminals and believe that they can get away with it.[85] It is hard to make a distinction between financial and political motivation behind a cyber activity, which can be any of the following: cybercrime, cyberterrorism and cyberwarfare. The difference between them is negligible.[86]

Furthermore, another solution to the problem that was suggested involved the Department of Defense conducting an "assessment of the risk to Information Systems stemming from cybercrime."[87] This panelist believes that a rigorous valuation of the likelihood of cybercriminal action against its assets as well as the consequences of such action in order to properly prioritize protection efforts, response options, and other policy actions is necessary at this point for the DoD.[88]

Lastly, one of the panelists suggested that the DoD can reduce the consequence of cybercrimes through better cyber hygiene, including better monitoring, greater network segmentation, and rigorous least-privilege, in which the authentication is granted to authorized

users in a "Need-to-Know" context, but no more than that.[89] All of these recommendations tremendously decrease the risks from malicious software that can take complete control over a computer or an entire network. This solution was stressed with the rationale that the cybercrimes do not have to be consequential if they can be detected and defeated early in their cycle or if the compromise of some systems does not lead to the compromise of all systems.[90] All of the solutions suggested by the panelists were innovative, effective and feasible.

During the second round, each panelist reviewed all the suggested solutions they developed during the brainstorming first round. They ranked one solution as the most feasible and effective and a second one as an alternative solution. As a result, two solutions suggesting transnational cooperation were eliminated due to the low endorsement of 20 percentage approvals. Additionally, no one favored resourcing the requirements of a cyber deterrence policy.

The third round consisted of only two of the suggested solutions as 90 percent of all the panelists selected them either as a highly recommended solution or as an alternative solution. During this round, most panelists moved toward consensus on one solution. Others favored the solution of sharing and understanding adversary TTPs. Further details about each round have been provided in Appendix D.

Analysis of the Delphi Study Results

The claim emphasizing a transnational cooperation with EU defense and/or law enforcement agencies was not a favorable context factor for the majority of experts that participated in the Delphi study. The study has investigated the feasibility and effectiveness of such collaboration; for example, partnership with Europol's EC3. The entreaty stressing the significance of transnational collaboration is an important element to overcome the political, law

enforcement, and cyber forensic challenges the DoD could face in isolating the threat actor. At the present time, cybercriminals and Advanced Persistent Threat (APT) actors, who are hackers with espionage and political motives and carry out highly sophisticated cyberattacks, share tools and tactics. Thus, the potential of a non-state cybercriminal to initiate a catastrophic cyberattack against the U.S. homeland should not be overlooked. Leveraging of the intra-coalition resources such as sharing of tactics, techniques and procedures used by adversaries are not only a valuable force multiplier for an effective cyber defense but also an efficient way to combat cybercrime and increasing resiliency. In addition, it improves the capability of Department of Defense's digital forensic tools in deterring and responding to online threats. This coalition cooperation could open the door to advance a clearinghouse for significant malicious cyber-enabled activities where TTPs used by adversaries can be shared between the law enforcement agencies and DoD, paving the path for standardizing reporting data, and establishing other clearinghouses in other parts of the world.[91]

Although a solution leveraging the proper transnational cooperation approach was given to the Delphi study panelists, the majority of the experts disagreed with it. There are two reasons for this disagreement. First, "understanding adversary TTPs" is important in the long run. However, before the attainment of sharing TTPs in real time, it is important that the DoD consider the science that conveys it, which TTPs are "stable and indicative," and which fluctuates from one attack to the other. For example, one may think of all the work done in biometrics to differentiate usable biometrics from unusable ones that yielded the current consensus that fingerprints are the gold standard.[92] Similarly, if U.S. Department of Defense could acquire valuable digital footprint of cyber activity, a collection of bilateral exchanges with European Union's law enforcement agencies is of limited use when compared to a collection of

multilateral exchanges of a broader coalition of potential targets or a central clearinghouse (or several such clearinghouses).[93] For that effort, governments must collaborate globally to develop an effective model to successfully fight cybercrime.

Second, "attribution" is useful only if one is attacked by criminals who are subject to extradition. It allows a strong case to be taken against the perpetrator. However, those who could successfully carryout a cyberattack, cyberterrorism, or cyberespionage against the DoD in all probability work for a state such as Russia or China, or a non-state group such as Al Qaeda, Hezbollah or ISIL. In such a situation, it is highly unlikely an adversary would give up their hackers so that (U.S.) justice will be served upon them. For example, Evgeniy Mikhailovich Bogachev of Russia is one of the FBI's most wanted hackers, and lives in Russia. He is the creator of Zeus, also known as GOZ malware that has been used to steal more than $100 million from bank accounts.[94] Later, evidence showed modified instances of GOZ was used against the governments of Ukraine, Georgia and Turkey for espionage purposes that were in the interest of the Russian government.[95] Several popular and credible sources used in this study speculate that as long as a black hat Russian hacker does not commit cybercrime against Russia, the Russian government will protect them, as well as contract hire the Russian Federal Security Service (FSB).[96]

A final point one of the Delphi study panelists made in the argument against attribution as a solution is that if the United States carries out cyber espionage against other countries, then the U.S. can expect other countries to carry out cyber espionage against it. In that case, what good does the attribution do? Regardless of these challenges, attribution in cyberspace is important. Attribution is a critical step in countering an attack of your adversary; especially when hostile cyber acts were conducted by an enemy state in response to the United States'

application of Diplomatic, Informational, Military, and Economic (DIME) Instruments of Power (IOPs) against the enemy's will. When it comes to attribution, the United States recognizes hostile cyber activities which "constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law."[97] However, with a global-level accord on what is the acceptable use of Internet, attribution can be more effective.

For all intents and purposes, this study suggests that the U.S. Department of Defense's collaboration with EU counterpart or law enforcement agencies such as EC3 is not an effective solution to combat cybercrime, cyberterrorism. Though, this study indicated that in the long run, multilateral TTP exchanges of a larger world body and a central clearinghouse or multiple clearinghouses will be an effective solution.

The majority of panelists agreed that in order to properly prioritize protection efforts, response options, and other policy actions including facilitating collaboration between countries, the U.S. Department of Defense should assess risks to Information Systems resulting from Cybercrime. In their view, it is an effective, as well as a realistic solution. A risk assessment can be done in a short period of time in comparison to all the other suggested solutions presented during this study (see Appendix D).

Recommendation

At the Department of Defense, risk assessment of Information Systems has always been an ongoing process. Every Service has well established guidance, methodology, frameworks and standardized tools to calculate risk levels. Given the Department of Defense's current capabilities and approach such as its never ending loop of risk assessment process of discovering and correcting security vulnerabilities, and preventing security breaches, why would the solutions offered by a Delphi study panelist make much of difference? This solution stresses that

the dynamic nature of cyberspace involves a dynamic strategy. Thus, effectively combating cybercrime requires the risk-informed security strategy. To that end, the above question is outside the scope of this study, and the author recommends that the DoD investigate it further.

Section 6: Conclusion

Annual cybercrime statistics data shows that the cybercrime is on the rise, which means victim nations are not doing their part to identify their cybercrime actors as these criminal actors know their targets. *The Art of War* by Sun Tzu reminds us "If you know yourself but not the enemy, for every victory gained you will also suffer a defeat… If you know neither the enemy nor yourself, you will succumb in every battle."[98] Nations joined to battle pirates attacking merchant ships near the East African coasts, or permitted naval ships in major waterways to safeguard the economic security through protecting the sea-lanes. Likewise, to establish a sustainable cybersecurity and cyber deterrence, it is important that the DoD be a part of the multilateral institutions that work together to enhance cyber security. This collaboration enables the sharing of critical information such as tactics, techniques and procedures used by adversaries. It can also help the Department of Defense to improve the efficiency and effectiveness of cyber forensic tools to isolate malicious actors. However, this study found that the effectiveness of such collaboration lies in the exchanges that happen in a broader coalition of potential targets of cybercrime, and such effort is a long run solution. It observed that the collaboration with EU law enforcement such as the United Kingdom's National Crime Agency (NCA), European Defense Agency (EDA), and Europol's EC3 or Joint Cybercrime Action Taskforce (J-CAT) would not essentially help to increase the DoD's capacity on the offensive side to discourage the malicious cyber actor. Instead, the study concluded that in order to effectively maintain the U.S. national security and economic strength through safeguarding cyberspace, DoD ought to become

accustomed to a risk-informed security strategy specifically involving the assessment of risks to Information Systems resulting from Cybercrime. It would also help to create a realistic and effective cyber-deterrence strategy.

This study agrees with the assertion that the collective effort by a large body of the international community in sharing TTPs can be valuable to understanding their common enemy as well as in building a sustainable security program and understanding how their adversaries operate. However, it finds that such collaboration may be valuable in the long run. In *The Unruled World,* Stewart Patrick stressed that the conventional deterrence and retaliatory conventional punishment methods may not be an option in the event of a cyberattack because "determining the location of the attacker is extremely resource intensive and hard to prove as the attacker can route the attack through anonymizing computers to avoid being detected."[99, 100] As the Cloud is becoming a globally accepted cyber technology, sophisticated hackers focus on the exploitation of Cloud based systems for greater anonymity and larger return because they see Cloud as "a fruit-bearing jackpot."[101] In order to properly prioritize the DoD Information Systems protection efforts, response options, and other policy actions, DoD must assess risks to Information Systems resulting from Cybercrime. As this assessment also weighs odds and magnitudes of penetration, a risk-informed Information Systems security strategy can be derived. The study concluded that this effort is the most effective short run solution for the U.S. Department of Defense to prevent cybercrimes of significant consequence.

Appendix A

Seeking Research Participants for Delphi Study (Amended 08 March 2016)

Hello,

My name is Roby Valiaveedu. I plan to conduct a research study to discover the benefits of the United States Department of Defense (DoD) participating in a multinational Cybercrime Joint Task Force, specifically with the nations that are part of the Council of Europe Convention on Cybercrime (CEC) and European Cybercrime Centre (EC3) to be more effective in digital forensic investigation to curb down cybercrimes. I am writing this email to inquire if you would be interested in participating in my research study.

The study will require 15-20 participants who are either subject matter experts in the areas of political science, international relations, and information security or White Hat hackers who work for leading information technology security companies as well as several high ranking civilians and officers within USAF who are cyber-domain subject matter experts. You were chosen to consider participation because you fulfilled these criteria.

Participation will entail the following:
Phase one: Brainstorming- responding to an email in one to two sentences regarding one specific question on cybercrime
Phase two: Evaluation- Re-evaluating your answer from phase one in light of other participants' response
Phase three: Consensus- Respond to final email to obtain a consensus.

The participants are kept anonymous to each other throughout the process. Participants will have four days' time to responds to the email sent each Monday evening (staring March 14, 2016 ending on April 01 2016)

I would especially appreciate your willingness to share your important thoughts and insights into this study. If you are interested in participating in this study, kindly respond to this email before March 11, 2016. Also I would appreciate any other leads for participation in this study.

V/r,
Roby Valiaveedu

Appendix B

Delphi Study on Reducing Cybercrime and Increasing Cyber Defense: Round1 (Amended 21 March 2016)

Dear participant,

Thank you for your participation in this Delphi study. The purpose of this study is to find effective and practical solutions to the problem of increased sophistication and frequency of cyberattacks against U.S. organizations. To find solutions for effective combating, prevention, deterrence and detection of potential cyberattacks, the following question is posed to you:

What could help the U.S. Department of Defense (DoD) to prevent cybercrimes of significant consequence, especially with the rapid increase in Cloud computing?

Please provide a solution statement and its rationale. The proposed solution statement(s) should be something that can be doable in a short period of time in comparison to the proposal of UN Cyberspace Treaty, which could take a decade or more of negotiations.

Solution Statement	Rationale
The DoD can be more effective in its digital forensic by collaborating and partnering with Europol's European Cybercrime Centre (EC3). This expanded information sharing cooperation will help to effectively trace the physical source of an attack on a near real-time basis. Thus, provides an opportunity for attribution.	This proper transnational cooperation would ensure the rapid flow of information and evidence while windows of opportunity are still open to identify the perpetrator and assist in taking required countermeasures.

Kindly respond to this email before Friday, March 25, 2016. Again, thank you.

V/r,
Roby Valiaveedu

Appendix C

Delphi Study on Reducing Cybercrime and Increasing Cyber Defense: Round 2 (Amended 03 April 2016)

Dear Participant,

This questionnaire is part of a Master's Degree Program research project that lasts for eight weeks, being conducted as a Delphi study in three rounds. Most of you have already completed the first round; this is the second round. **Please enter a numeric priority for two of the most feasible and effective solution statements/rationale listed below. Enter "1" for the top solution, and "2" for the (top) alternative solution.** Some of you may not find your exact wordings or the solution\rationale statement in this consolidated list because two or more panelists conveyed the same message. If your opinion has changed or been influenced by the feedback, you may revise your previous answers for clarity without losing the message in it or add an additional row if you wish. We're looking for a solution that is innovative.

I hope to receive your completed questionnaire before Friday, April 8th. Please do not select more than two solutions below.

Entry #	How Important? (Enter 1 or 2)	Solution Statement	Rationale
1		The DoD can be more effective in its digital forensic by collaborating and partnering with Europol's European Cybercrime Centre (EC3). This expanded information sharing cooperation will help to effectively trace the physical source of an attack on a near real-time basis. Thus, provides an opportunity for attribution.	This proper transnational cooperation would ensure the rapid flow of information and evidence while windows of opportunity are still open to identify the perpetrator and assist in taking required countermeasures.

2		The DoD can reduce the consequence of cybercrimes through better cyber hygiene, including better monitoring, greater network segmentation, and rigorous least-privilege.	Cybercrimes do not have to be consequential if they can be detected and defeated early in their cycle or if the compromise of some systems does not lead to the compromise of all systems.
3		The DoD can reduce the incidence of cybercrimes by resourcing the requirements of a cyber deterrence policy.	Countries that protect their cybercriminals and believe th/// *[that they can get away with it]*
4		DoD should conduct an assessment of the risk to information systems stemming from cybercrime	DoD needs a rigorous assessment of the likelihood of cybercriminal action against its assets as well as the consequences of such action in order to properly prioritize protection efforts, response options, and other policy actions
5		Leveraging the Cloud to facilitate collaboration between countries with an emphasis on sharing Tactics, Techniques and Procedures (TTPs) used by adversaries between the DoD and/or Law Enforcement (LE).	A Cloud solution would provide a medium where DoD and/or LE could more rapidly respond to multi-national crimes. Sharing TTPs in real time would help improve LE's ability to recognize and respond to threats more efficiently.

Appendix D

Delphi Study on Reducing Cybercrime and Increasing Cyber Defense: Round 3 (Amended 09 April 2016)

Dear Participant,

This is the final round of this Delphi study. I removed the solution statements that received the least number of endorsements. Percentages of the ranking for the top two solutions/rationales are provided in the respective column. Please take another look, and let me know if you answer changed. I am attaching your previous round 2 answers to this email. If you do not find the solution\rationale that you have endorsed during the second round, and you cannot agree with any of the given solution statement\rationale below, please select "I disagree." Please do not select more than one solution below.

Please respond by Tuesday, April 12th.

Top Solution	Alternative Solution	Top Final Pick (1)	Solution Statement	Rationale
20%	40%		The DoD can reduce the consequence of cybercrimes through better cyber hygiene, including better monitoring, greater network segmentation, and rigorous least-privilege.	Cybercrimes do not have to be consequential if they can be detected and defeated early in their cycle or if the compromise of some systems does not lead to the compromise of all systems.
60%	20%		DoD should conduct an assessment of the risk to information systems stemming from cybercrime	DoD needs a rigorous assessment of the likelihood of cybercriminal action against its assets as well as the consequences of such action in order to properly prioritize protection efforts, response options, and other policy actions
20%			I disagree	

Thank you.

V/r,

Roby Valiaveedu

Delphi Study on Reducing Cybercrime and Increasing Cyber Defense: Final Result

Top Solution	Alternative Solution	Top Final Pick (1)	Solution Statement	Rationale
	20%		The DoD can be more effective in its digital forensic by collaborating and partnering with Europol's European Cybercrime Centre (EC3). This expanded information sharing cooperation will help to effectively trace the physical source of an attack on a near real-time basis. Thus, provides an opportunity for attribution.	This proper transnational cooperation would ensure the rapid flow of information and evidence while windows of opportunity are still open to identify the perpetrator and assist in taking required countermeasures.
20%	**40%**		The DoD can reduce the consequence of cybercrimes through better cyber hygiene, including better monitoring, greater network segmentation, and rigorous least-privilege.	Cybercrimes do not have to be consequential if they can be detected and defeated early in their cycle or if the compromise of some systems does not lead to the compromise of all systems.
			The DoD can reduce the incidence of cybercrimes by resourcing the requirements of a cyber deterrence policy.	Countries that protect their cybercriminals and believe that they can get away with it
60%	**40%**	**1**	DoD should conduct an assessment of the risk to Information Systems stemming from cybercrime	DoD needs a rigorous assessment of the likelihood of cybercriminal action against its assets as well as the consequences of such action in order to properly prioritize protection efforts, response options, and other policy actions

20%			Leveraging the Cloud to facilitate collaboration between countries with an emphasis on sharing Tactics, Techniques and Procedures (TTPs) used by adversaries between the DoD and/or Law Enforcement (LE).	A Cloud solution would provide a medium where DoD and/or LE could more rapidly respond to multi-national crimes. Sharing TTPs in real time would help improve LE's ability to recognize and respond to threats more efficiently.
		20%	I disagree	

Appendix E

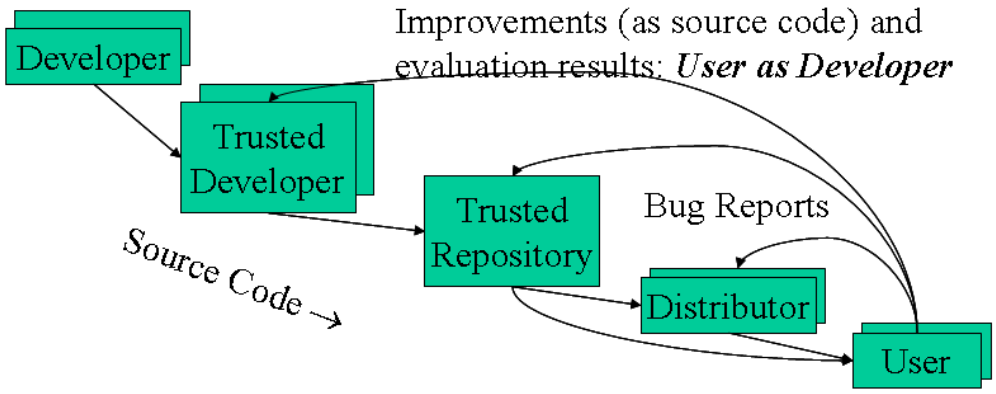

Figure: 2.2.1
Open Source Software (OSS) development - collaborative process.[102]

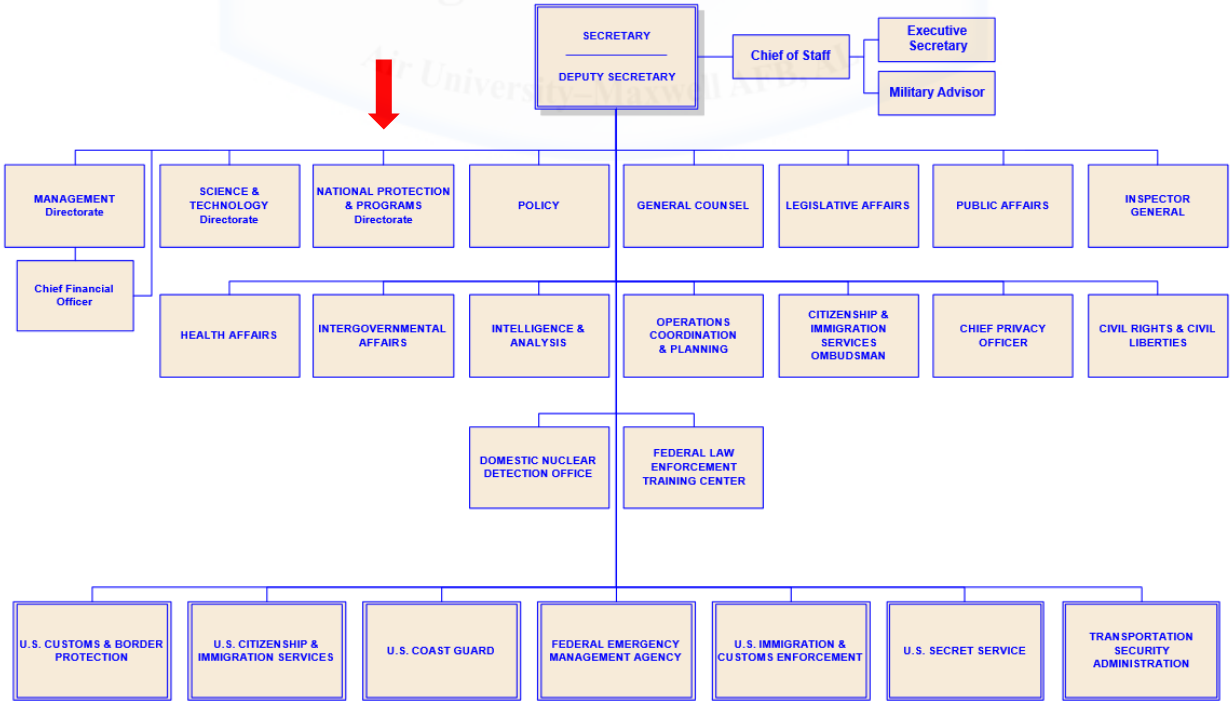

Figure: 2.2.1.1
The Department of Homeland Security (DHS) Organizational Chart.[103]

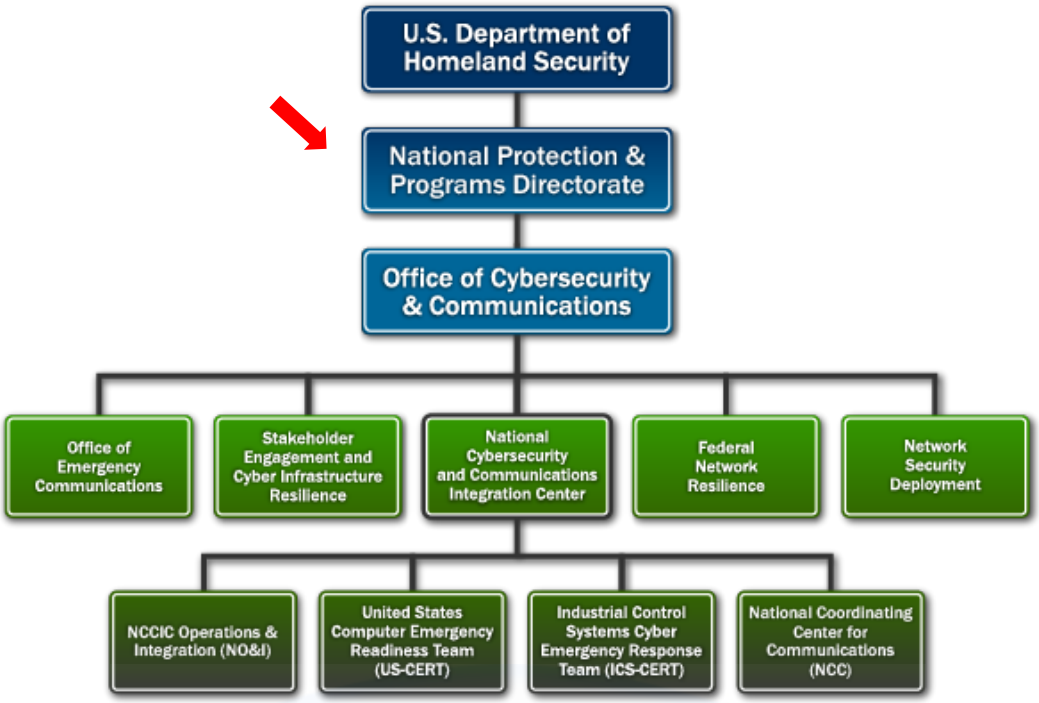

Figure: 2.2.1.2
National Cybersecurity and Communications Integration Center (NCCIC) Organizational Chart.[104]

Endnotes

[1] Speiser, "This one map explains the entire worldwide economy," 1.
[2] Bradley, et al., "Internet of Everything (IoE) Value Index: How Much Value Are Private-Sector Firms Capturing from IoE in 2013?"
[3] Cisco Consulting Services, *The Internet of Everything—A $19 Trillion Opportunity*,2.
[4] Dean, et al., The Internet Economy in the G-20, The $4.2 Trillion Growth Opportunity."
[5] Europol, "OCTOPUS PROGRAMME - Threats, Trends and the Perspective of Europol," 2.
[6] Department of Defense, *Joint Publication (JP) 3-12: Cyberspace Operations*, GL-4.
[7] Ibid., I-6.
[8] Kissel, *Glossary of Key Information Security Terms*, 103.
[9] Ibid., 57.
[10] Royal Canadian Mounted Police, *Cybercrime: an overview of incidents and issues in Canada*, 3.
[11] Obama, *National Security Strategy*, ii.
[12] Verizon, *2015 Data Breach Investigations Report, Quantify the impact of a data breach with new data from the 2015 DBIR*, 6.
[13] Sanders IV, "Bitcoin: Islamic State's online currency venture."
[14] Kemp, "US Military Social Media Accounts Hacked by ISIS Sympathizers Cyber Caliphate."
[15] Burt, "Thousands of French Websites Face DDoS Attacks Since Charlie Hebdo Massacre."
[16] OpenView Ventures, "Global Cloud Computing Services Market to Reach US$127 Billion by 2017, According to New Report by Global Industry Analysts, Inc."
[17] Gaudin, "The move away from legacy IT will continue to fuel growth, Gartner says."
[18] Alert Logic, *Cloud Security Report*, 5.
[19] Smith, et al., *Cybercrime Risks and Responses, Eastern and Western Perspectives*, 159.
[20] Council on Foreign Relations, "The Global Regime for Transnational Crime."
[21] Ibid.
[22] Price Waterhouse and Coopers, "Global Economic Crime Survey 2016."
[23] Sumner, "Hackers see cloud as 'a fruit-bearing jackpot' for cyber attacks."
[24] U.S. Department of Justice, "Botnets 101 What They Are and How to Avoid Them."
[25] McDonald, et al., *Research Integration Using Dialogue Methods*, 41.
[26] United States Government Accountability Office. *GAO-10-606 Global Cybersecurity Challenges*, 36.
[27] European Police Office. *The Internet Organised Crime Threat Assessment (iOCTA)*, 49.
[28] Mandiant, *M-Trends 2015: A view from the front lines*, 3.
[29] White House. *International Strategy for Cyberspace - Protecting Our Networks: Enhancing Security, Reliability, and Resiliency*,18.
[30] Sofaer, et al., *Cyber security and international agreements, Proceedings of a Workshop on Deterring Cyberattacks, 179-182.*
[31] Department of Defense, *Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 3.
[32] Sofaer et al., The *Transnational Dimension of Cyber Crime and Terrorism*, 17.
[33] Central Intelligence Agency, "The World Factbook."
[34] Price Waterhouse and Coopers, "Global Economic Crime Survey 2016."

[35] Verizon, *2015 Data Breach Investigations Report, Quantify the impact of a data breach with new data from the 2015 DBIR,* 2.
[36] Ibid., 6.
[37] Gemalto *2014 Year of Mega Breaches & Identity Theft*, 7.
[38] Ponemon Institute, "2015 Cost of Cyber Crime Study: United States."
[39] Carbonnel, "Ex-Soviet hackers play outsized role in cyber crime world."
[40] Pagliery, "The Cybercrime Economy Half of American adults hacked this year."
[41] Ponemon Institute, "Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study."
[42] Griffiths, "Cybercrime costs the average U.S. firm $15 million a year."
[43] Obama, *National Security Strategy*, 1.
[44] Guinn II, "Why you should adopt the NIST Cybersecurity Framework," 1.
[45] Obama, *International Strategy for Cyberspace*, 20-21.
[46] The Department of Defense, *Quadrennial Defense Review Report,* 37.
[47] Garamone, "Cybercom Chief Discusses Importance of Cyber Operations."
[48] Chief Information Officer U.S. Department of Defense, "DoD Open Source Software (OSS) FAQ."
[49] Ibid.
[50] Obama, *International Strategy for Cyberspace*, 24.
[51] Department of Defense, *Quadrennial Defense Review Report*, 37-38.
[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] U.S. Department of Homeland Security, "National Cybersecurity and Communications Integration Center."
[56] Cooney, "GAO: Early look at fed's "Einstein 3" security weapon finds challenges."
[57] Ibid.
[58] Ibid.
[59] Pellerin, "DOD, DHS Join Forces to Promote Cybersecurity."
[60] U.S. Strategic Command, "U.S. Cyber Command."
[61] Department of Defense, *Quadrennial Defense Review Report*, 37-38.
[62] U.S. Strategic Command, "U.S. Cyber Command."
[63] U.S. Government Publishing Office (GPO), *United States Code, 2006 Edition, Supplement 4, Title 18 - CRIMES AND CRIMINAL PROCEDURE*, 298.
[64] Mandiant, *M-Trends 2015: A view from the front lines,* 23.
[65] Ibid.
[66] Council of Europe, "Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime."
[67] Archick, *Cybercrime: The Council of Europe Convention,* CRS-4.
[68] Sanchez, et al. "Terror cell warning as Europe scrambles to handle threats."
[69] American Civil Liberties Union, "Seven Reasons the US Should Reject the International Cybercrime Treaty."
[70] Grigsby, "Coming Soon: Another Country to Ratify the Budapest Convention."
[71] Ibid.
[72] Jeffray et al., *Underground web: the cybercrime challeng,* 8.
[73] Rayman, "The World's Top 5 Cybercrime Hotspots," 1.

[74] United Nations, "Delegates Consider Best Response to Cybercrime as Congress Committee Takes Up Dark Side of Advances in Information Technology," 1.
[75] Davidson, "Here's How Many Internet Users There Are."
[76] Internet World Stats, "World Internet Users and 2015 Population Stats."
[77] Cisco Systems, Inc., "Internet of Things (IoT)" 1.
[78] Price Waterhouse and Coopers, "Global Economic Crime Survey 2016," 1.
[79] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II*, 2.
[80] Obama, *National Security Strategy*, ii.
[81] National Institute of Standards and Technology, *NIST Cloud Computing Forensic Science Challenges*, 7.
[82] Ibid.
[83] Lawton, "Cloud computing crime poses unique forensics challenges."
[84] Libicki, Martin C. (Senior Management Scientist; Professor, Pardee RAND Graduate School, Santa Monica, CA), response to the Delphi study questionnaire from the author, 30 March 2016.
[85] Matthews, "Russia's Greatest Weapon May Be Its Hackers."
[86] Ibid.
[87] Schmidt, Lara. (Associate Director, RAND Project AIR FORCE, RAND Corporation, Santa Monica, CA), response to the Delphi study questionnaire from the author, 29 March 2016.
[88] Schmidt, Lara. (Associate Director, RAND Project AIR FORCE, RAND Corporation, Santa Monica, CA), response to the Delphi study questionnaire from the author, 29 March 2016.
[89] Libicki, Martin C. (Senior Management Scientist; Professor, Pardee RAND Graduate School, Santa Monica, CA), response to the Delphi study questionnaire from the author, 30 March 2016.
[90] Ibid
[91] Epley, Shown. (Chief, Infrastructure/Advanced Technology Branch, USAF), response to the Delphi study questionnaire from the author, 25 March 2016.
[92] Libicki, Martin C. (Senior Management Scientist; Professor, Pardee RAND Graduate School, Santa Monica, CA), response to the Delphi study questionnaire from the author, 10 April 2016.
[93] Ibid.
[94] Stevenson, "The Russian government may be protecting the creator of the world's most infamous malware."
[95] Ibid.
[96] Matthews, "Russia's Greatest Weapon May Be Its Hackers."
[97] Koh, "International Law in Cyberspace."
[98] Tzu, *The Art of War*, III.
[99] Patrick, "The Unruled World: The Case for Good Enough Global Governance."
[100] Valiaveedu, "Assessing Cyber Security Issues," 3.
[101] Sumner, "Hackers see cloud as 'a fruit-bearing jackpot' for cyber attacks," 1.
[102] Chief Information Officer U.S. Department of Defense, "DoD Open Source Software (OSS) FAQ," 1.
[103] Department of Homeland Security, "Organizational Chart," 1.
[104] Department of Homeland Security, "National Cybersecurity and Communications Integration Center," 1.

Bibliography

Alert Logic. *Cloud Security Report.* Houston, TX: Alert Logic, Inc., 2015. http://faculty.washington.edu/blabob/bob/Docs/2015%20Cloud%20Security%20Report.pdf

American Civil Liberties Union. "Seven Reasons the US Should Reject the International Cybercrime Treaty" New York, NY: November 2003. https://www.aclu.org/seven-reasons-us-should-reject-international-cybercrime-treaty (accessed 24 March 2016).

Archick, Kristin. *Cybercrime: The Council of Europe Convention,* Congressional Research Service, Washington, D.C.: The Library of Congress, CRS Report for Congress, July 22, 2004. http://fpc.state.gov/documents/organization/36076.pdf (accessed 03 March 2016).

Bradley, Joseph, Jeff Loucks, James Macaulay and Andy Noronha. "Internet of Everything (IoE) Value Index: How Much Value Are Private-Sector Firms Capturing from IoE in 2013?" *Cisco.com,* San Jose, CA: February 2013. http://ioeassessment.cisco.com/explore/full#/country/usa (accessed 16 March 2016)

Burt, Chris. "Thousands of French Websites Face DDoS Attacks Since Charlie Hebdo Massacre" West Chester, Ohio: Web Host Industry Review, 15 January 2015. http://www.thewhir.com/web-hosting-news/thousands-french-websites-face-ddos-attacks-since-charlie-hebdo-massacre (accessed 23 March 2016).

Carbonnel, Alissa De. "Ex-Soviet hackers play outsized role in cyber crime world" *reuters.com,* Moscow, Russia: 22 August 2013. http://www.reuters.com/article/net-us-russia-cybercrime-idUSBRE97L0TP20130822 (accessed 30 March 2016).

Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II.* Washington, D.C.: mcafee, 2014. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf (accessed 13 March 2016).

Central Intelligence Agency. "The World Factbook," *cia.gov* Washington, D.C.: Office of Public Affairs, March 2015. https://www.cia.gov/library/publications/resources/the-world-factbook/rankorder/2153rank.html#us (accessed 05 March 2016).

Chief Information Officer U.S. Department of Defense. "DoD Open Source Software (OSS) FAQ." Washington, D.C.: Pentagon, 2010. http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx (accessed 11 April 2016).

Cisco Consulting Services, *The Internet of Everything—A $19 Trillion Opportunity.* San Jose, CA: January 2014. http://www.cisco.com/c/dam/en_us/services/portfolio/consulting-services/documents/consulting-services-capturing-ioe-value-aag.pdf (accessed 16 March 2016).

Cisco Systems, Inc. "Internet of Things (IoT)" San Jose, CA: Cisco Systems, Inc., 2016. http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html (accessed 16 March 2016).

Cooney, Michael. "GAO: Early look at fed's "Einstein 3" security weapon finds challenges." Network World, 9 July 2015. http://www.networkworld.com/article/2946040/security0/gao-early-look-at-feds-einstein-3-security-weapon-finds-challenges.html (accessed 28 March 2016).

Council of Europe. "Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime." *CoE.int*, Strasbourg, France: Treaty Office, 16 March 2016. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (accessed 03 March 2016).

Council on Foreign Relations. "The Global Regime for Transnational Crime" *CFR.org*, New York, NY: 25 June 2013. http://www.cfr.org/transnational-crime/global-regime-transnational-crime/p28656 (accessed 23 March 2016).

Davidson, Jacob. "Here's How Many Internet Users There Are" *TIME*, New York, NY: Time Inc., 26 May 2015. http://time.com/money/3896219/internet-users-worldwide/ (accessed 16 March 2016).

Dean, David, Sebastian DiGrande, Dominic Field, Andreas Lundmark, James O'Day, John Pineda, and Paul Zwillenberg. "The Internet Economy in the G-20, The $4.2 Trillion Growth Opportunity" *bcgperspectives.com* San Francisco, CA: The Boston Consulting Group, 19 March 2012. https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_Internet_economy_g20/ (accessed 16 March 2016).

Department of Defense. *Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* Washington, D.C.: 2011. http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf (accessed 05 March 2016).

Department of Defense. *Joint Publication (JP) 3-12: Cyberspace Operations*, Joint Staff, Washington, D.C.: DoD, 5 February 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed 16 March 2016).

Department of Defense. *Quadrennial Defense Review Report*, Washington D.C.: February 2010. http://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf (accessed 30 March 2016).

Department of Homeland Security. "National Cybersecurity and Communications Integration Center" *dhs.gov*, Washington D.C.: DHS, January 2016. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center (accessed 08 April 2016).

Department of Homeland Security. "Organizational Chart" *dhs.gov*, Washington D.C.: DHS, July 2015. https://www.dhs.gov/organizational-chart (accessed 08 April 2016).

European Police Office. *The Internet Organised Crime Threat Assessment (iOCTA),* The Hague, NLD: European Police Office, 2014. https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf (accessed 05 March 2016).

Europol. "OCTOPUS PROGRAMME - Threats, Trends and the Perspective of Europol" Strasbourg, France: November 2011. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2476 (accessed 18 March 2016).

Garamone, Jim. "Cybercom Chief Discusses Importance of Cyber Operations" *DoD News* National Harbor, MD: Defense Media Activity, 14 April 2015. http://www.defense.gov/News-Article-View/Article/604453/cybercom-chief-discusses-importance-of-cyber-operations (accessed 30 March 2016).

Gaudin, Sharon. "The move away from legacy IT will continue to fuel growth, Gartner says" *Computerworld* 26 January 2016. http://www.computerworld.com/article/3026396/cloud-computing/global-public-cloud-market-expected-to-hit-204b-in-2016.html (accessed 10 March 2016).

Gemalto. *2014 Year of Mega Breaches & Identity Theft.* Belcamp, MD: 2014. http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf (accessed 16 March 2016).

Griffiths, James. "Cybercrime costs the average U.S. firm $15 million a year" *cnn.com,* New York, NY: CNNMoney, 8 October 2015. http://money.cnn.com/2015/10/08/technology/cybercrime-cost-business/ (accessed 16 March 2016).

Grigsby, Alex. "Coming Soon: Another Country to Ratify the Budapest Convention" New York, NY: 11 December 2014. http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/ (accessed 23 March 2016).

Guinn II, Jim. *Why you should adopt the NIST Cybersecurity Framework.* New York City, NY: PWC, May 2014. https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf (accessed 30 March 2016).

Internet World Stats. "World Internet Users and 2015 Population Stats" Bogota, Colombia: 30 November 2015. http://www.internetworldstats.com/stats.htm (accessed 16 March 2016).

Jeffray, Calum and Tobias Feakin. *Underground web: the cybercrime challenge.* The Australian Strategic Policy Institute Limited, Barton ACT, AUS: 2015. https://www.aspi.org.au/publications/underground-web-the-cybercrime-challenge/SR77_Underground_web_cybercrime.pdf (accessed 23 March 2016).

Kemp, Cheryl. "US Military Social Media Accounts Hacked by ISIS Sympathizers Cyber Caliphate" West Chester, Ohio: Web Host Industry Review, 13 January 2015. http://www.thewhir.com/web-hosting-news/us-military-social-media-accounts-hacked-isis-sympathizers-cyber-caliphate (accessed 23 March 2016).

Kissel, Richard. "Glossary of Key Information Security Terms," NISTIR 7298, National Institute of Standards and Technology, Computer Security Division Information Technology Laboratory, Gaithersburg, MD: U.S. Department of Commerce, May 2013. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913810 (accessed 15 March 2016).

Koh, Harold Hongju. "International Law in Cyberspace" Legal Advisor U.S. Department of State, Ft. Meade, MD: USCYBERCOM Interagency Legal Conference, 18 September 2012. http://www.state.gov/s/l/releases/remarks/197924.htm (accessed 12 April 2016).

Lawton, George. "Cloud computing crime poses unique forensics challenges," *techtarget.com*, San Francisco, CA: searchcloudcomputing.com, January 2011. http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges (accessed 16 March 2016).

Mandiant. *M-Trends 2015: A view from the front lines*. Alexandria, VA: 2015. https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf (accessed 05 March 2016).

Matthews, Owen. "Russia's Greatest Weapon May Be Its Hackers" *Newsweek.com*, New York, NY: Newsweek, 7 May 2015. http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html (accessed 06 April 2016).

McDonald, David, Gabriele Bammer and Peter Deane. *Research Integration Using Dialogue Methods*, The Australian National University, Canberra, AU: ANU E Press, 2009.

National Institute of Standards and Technology. *NIST Cloud Computing Forensic Science Challenges.* NIST Cloud Computing Forensic Science Working Group Information Technology Laboratory, Gaithersburg, MD: U.S. Department of Commerce, June 2014. http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf (accessed 16 March 2016).

Obama, Barack. *International Strategy for Cyberspace*, Washington D.C.: The White House, February 2015. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 30 March 2016).

Obama, Barack. *National Security Strategy*, Washington D.C.: The White House, February 2015.

OpenView Ventures. “Global Cloud Computing Services Market to Reach US$127 Billion by 2017, According to New Report by Global Industry Analysts, Inc.” *openviewpartners.com* Boston, MA: OpenView Venture Partners, April 2015. http://openviewpartners.com/news/global-cloud-computing-services-market-to-reach-us127-billion-by-2017-according-to-new-report-by-global-industry-analysts-inc/ (accessed 15 March 2016)

Pagliery, Jose. “The Cybercrime Economy Half of American adults hacked this year” *cnn.com,* New York, NY: CNNMoney, 28 May 2014. http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/ (accessed 16 March 2016).

Patrick, Stewart. “The Unruled World: The Case for Good Enough Global Governance,” *Foreign Affairs* 93, no. 1, January/February 2014. https://www.foreignaffairs.com/articles/2013-12-06/unruled-world (accessed 16 March 2016).

Pellerin, Cheryl. “DOD, DHS Join Forces to Promote Cybersecurity” Washington D.C.: American Forces Press Service, 13 October 2010. http://archive.defense.gov/news/newsarticle.aspx?id=61264 (accessed 28 March 2016).

Ponemon Institute. “2015 Cost of Cyber Crime Study: United States,” *ponemon.org,* Traverse City, MI: MacKenzie Marketing Group, 7 May 2015. http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states (accessed 16 March 2016).

Ponemon Institute. “Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study,” *ponemon.org,* Traverse City, MI: MacKenzie Marketing Group, 7 May 2015. http://www.ponemon.org/news-2/66 (accessed 16 March 2016).

Price Waterhouse and Coopers. “Global Economic Crime Survey 2016,” *pwc.com*, New York City, NY: PWC, 2016. http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html (accessed 03 March 2016).

Price Waterhouse and Coopers. “Global Economic Crime Survey 2016” New York City, NY: PWC, 2016. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.html (accessed 03 March 2016).

Rayman, Noah. “The World’s Top 5 Cybercrime Hotspots,” *TIME,* New York, NY: Time Inc., Aug. 7, 2014. http://time.com/3087768/the-worlds-5-cybercrime-hotspots/ (accessed 06 April 2016).

Royal Canadian Mounted Police. *Cybercrime: an overview of incidents and issues in Canada.* Ottawa ON, Canada: RCMP National Headquarters, 2014. http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-eng.pdf (accessed 23 March 2016).

Sanchez, Ray, Laura Smith-Spark, and Jethro Mullen. “Terror cell warning as Europe scrambles to handle threats,” *cnn.com*, 16 January2015. http://www.cnn.com/2015/01/16/europe/europe-terrorism-threat/ (accessed 03 March 2016).

Sanders IV,Lewis. “Bitcoin: Islamic State’s online currency venture” *Deutsche Welle*, Bonn, Germany: 20 September 2015. http://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856 (accessed 23 March 2016).

Smith, Russell G., Ray Chak-Chung Cheung and Laurie Yiu-Chung Lau. *Cybercrime Risks and Responses, Eastern and Western Perspectives,* New York, NY: Palgrave Macmillan, September 2015.

Sofaer, Abraham and Seymour Goodman, *The Transnational Dimension of Cyber Crime and Terrorism,* Stanford, CA: Hoover Institution Press, 2001. http://onlinebooks.library.upenn.edu/webbin/metabook?id=hoovercyber (accessed 23 March 2016).

Sofaer, Abraham, David Clark, and Whitfield Diffie. *Cyber security and international agreements, Proceedings of a Workshop on Deterring Cyberattacks*, Washington, D.C.: National Academy of Sciences, 2009. http://www.nap.edu/read/12997/chapter/13#182 (accessed 05 March 2016).

Speiser, Matthew. “This one map explains the entire worldwide economy” *businessinsider.com*, 21 July 2015. http://www.businessinsider.com/this-one-map-explains-the-entire-worldwide-economy-2015-7 (accessed 16 March 2016).

Stevenson, Alastair. “The Russian government may be protecting the creator of the world’s most infamous malware” *Business Insider Inc*. New York, NY 6 Aug 2015. http://www.businessinsider.com/gameover-zeus-alleged-author-may-be-getting-help-from-the-russian-government-2015-8?r=UK&IR=T (accessed 11 April 2016).

Sumner, Stuart. “Hackers see cloud as ‘a fruit-bearing jackpot’ for cyber attacks” *Computing*, London, UK: Incisive Media, 6 October 2015. http://www.computing.co.uk/2429256 (accessed 16 March 2016).

Tzu, Sun. *The Art of War*, The Internet Classics Archive by Daniel C. Stevenson, Web Atomics, Cambridge, MA: classics.mit.edu. http://classics.mit.edu/Tzu/artwar.html (accessed 16 March 2016).

U.S. Department of Homeland Security (DHS). “National Cybersecurity and Communications Integration Center” November, 2015. https://www.hsdl.org/?view&did=780083 (accessed 28 March 2016).

U.S. Department of Justice. “Botnets 101 What They Are and How to Avoid Them,” News Blog, *FBI.gov* Washington, D.C.: 05 June 2013. https://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them (accessed 16 March 2016).

U.S. Government Publishing Office (GPO). *United States Code, 2006 Edition, Supplement 4, Title 18 - CRIMES AND CRIMINAL PROCEDURE*. Washington, D.C., 7 January 2011. https://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-sec1030.pdf (accessed 28 March 2016).

U.S. Strategic Command. "U.S. Cyber Command" Offutt Air Force Base, NE: 2016. https://www.stratcom.mil/factsheets/2/Cyber_Command/ (accessed 28 March 2016).

United Nations. "Delegates Consider Best Response to Cybercrime as Congress Committee Takes Up Dark Side of Advances in Information Technology" 12th UN Congress on Crime Prevention and Criminal Justice Committee II, Salvador, Brazil: 13 April 2010. http://www.un.org/press/en/2010/soccp349.doc.htm (accessed 31 March 2016).

United States Government Accountability Office. *GAO-10-606 Global Cybersecurity Challenges*, Washington, D.C.: GAO, 2010. http://gao.gov/assets/310/308401.pdf (accessed 07 March 2016).

Valiaveedu, Roby. "Assessing Cyber Security Issues" Maxwell AFB, AL: The United States Air Force Air Command and Staff College, 09 November 2015.

Verizon. *2015 Data Breach Investigations Report, Quantify the impact of a data breach with new data from the 2015 DBIR.* Basking Ridge, NJ: Verizon Enterprise, 2015. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf (accessed 23 March 2016).

White House. *International Strategy for Cyberspace - Protecting Our Networks: Enhancing Security, Reliability, and Resiliency,* Washington D.C.: The White House, 2011.