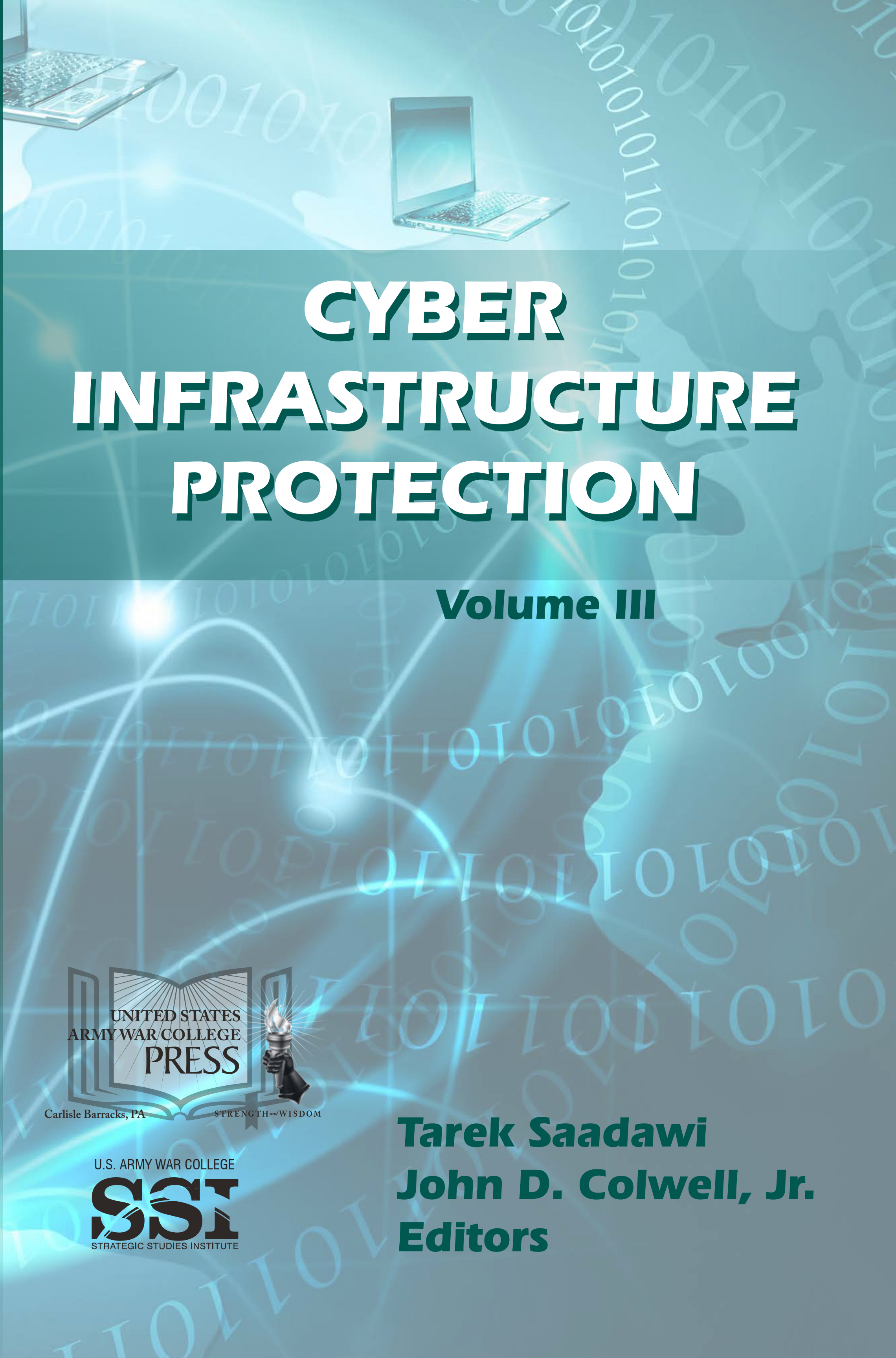


CYBER INFRASTRUCTURE PROTECTION

Volume III

UNITED STATES
ARMY WAR COLLEGE
PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

Tarek Saadawi
John D. Colwell, Jr.
Editors

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

CYBER INFRASTRUCTURE PROTECTION
VOLUME III

Tarek Saadawi
John D. Colwell, Jr.

Editors

June 2017

The views expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of certain reports may also be obtained free of charge while supplies last by placing an order on the SSI website. Check the website for availability. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: *ssi.armywarcollege.edu.*

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a quarterly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at the following address: *ssi.armywarcollege.edu/newsletter/.*

ISBN 1-58487-753-7

CONTENTS

FOREWORD

Cyberspace, or the Internet, supports important commercial assets as well as non-commercial assets. A hacker, a state or nonstate agent, or a cybercriminal can attack cyberspace for financial, political, or espionage reasons, or to steal identities, or to cause the disruption of critical infrastructure.

We have achieved great advancement in computing systems in both hardware and software and their security. On the other hand, we still see massive cyberattacks that result in enormous data losses. Recent attacks have included sophisticated cyberattacks targeting many institutions, including those who provide management and host the core parts of Internet infrastructure. The number and types of attacks, the duration of attacks, and their complexity are all on the rise.

The Cyber Infrastructure Protection (CIP) colloquium for the academic year 2015-16 was focused on strategy and policy directions relating to cyberspace; and how those directions should deal with the fast-paced, technological evolution of that domain. Topics addressed by the colloquia included: a cooperative international deterrence capability as an essential tool in cybersecurity; an estimation of the costs of cybercrime; the impact of prosecuting spammers on fraud and malware contained in email spam; cybersecurity and privacy in smart cities; smart cities demand smart security; and, a smart grid vulnerability assessment using national testbed networks.

Our offerings here are the result of the 2015-16 CIP, conducted on October 15, 2015, by the Center of Information Networking and Telecommunications (CINT) at the Grove School of Engineering, the City

University of New York (CUNY) City College, and the Strategic Studies Institute (SSI) at the U.S. Army War College (USAWC). The colloquium brought together government, business, and academic leaders to assess the vulnerability of our cyber infrastructure and provide strategic policy directions for the protection of such infrastructure.

Given the complexities of national security in the 21st century and the fast-changing nature of the cyber domain, SSI proudly presents the results of this very relevant colloquium. We are sure it will be an essential read for both the practitioner and the academic alike to gain a better understanding of cybersecurity.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

PREFACE

This book is a follow-on to our earlier two books published in 2011 and 2013 respectively; and offers a detailed look at various aspects of cybersecurity. The chapters in this book are the result of invited presentations in a 1-day conference on cybersecurity that was held at the City University of New York (CUNY), City College, on October 15, 2015.

A key contribution of this book is that it provides an integrated framework and a comprehensive view of the various cyber infrastructure protection (CIP) approaches. The book is divided into three main parts: Part I addresses policy and strategy for cybersecurity and cybercrime; Part II focuses on the cybersecurity of smart cities; and, Part III discusses cyber infrastructure security and technical issues. We strongly recommend this book for policymakers and researchers.

PART I:

CYBERSECURITY POLICY, STRATEGY, AND CYBERCRIME

CHAPTER 1

CYBERSECURITY: A GOOD DEFENSE IS A COOPERATIVE INTERNATIONAL INTELLIGENT DETERRENCE CAPABILITY

Haidar Chamas
Tarek Saadawi

INTRODUCTION[1]

This chapter discusses the need to establish an International Cyber Union (ICU) to overcome cybersecurity challenges in securing cyber infrastructure. Recent cybersecurity attacks and breaches demonstrate the growing means of anonymous communication, sophistication, and boldness in conducting well-orchestrated cyberattacks. In order to combat growing cybersecurity threats, we must consider these events as urgent wake-up calls for the need to establish international cybersecurity laws, regulations, and standards. We recommend the establishment of an ICU to monitor, collect, and verify international cyber-illegalities and hacks, take necessary legal actions, and provide a platform for international cooperation in the cyber domain. The ideal ICU would be an international independent body that would oversee how to deal with addressing international cybercrimes, cyberattacks, cyberespionage, cybervandalism and sabotage, as well as cyberwarfare. The need to strengthen cybersecurity technologies with advanced mechanisms that help to identify where attacks originate from, and help to determine the attackers' identities, are becoming increasingly vital to ensure uninterruptible use of cyberspace. In addition, this chapter touches on a potential new threat of using cyber as a weapon by states. This chapter also proposes an organizational model for an ICU that will lead to increased collaboration and trust among nations and minimize cyber-security threats.

Cyberspace, or the Internet, is an open global communication infrastructure accessible by anyone to share, exchange, or to download information online. This infrastructure supports important commercial assets for conducting electronic transactions (e-commerce) globally as well as non-commercial transactions. Anyone connected to cyberspace can access the global network virtually from anywhere. As a state or nonstate agent, a cybercriminal can attack cyberspace for financial, political, or espionage reasons, or to steal identities or to cause the disruption of critical infrastructure. Cybersecurity is a protection mechanism for the information that is stored or transported through cyberspace.

Cybersecurity attacks continue to flourish, due in part to software errors, misconfigurations, unpatched operating systems and applications, or user errors, which make cyber systems susceptible to attacks or exploitation. Although the required technology needed to counter cyberattacks and to ensure secure information exists today, many organizations still do not have a cybersecurity strategy, nor do they allocate the required resources to tackle cyberattacks. Each organization must identify, prioritize, and implement the required policies to defend its most sensitive information and network infrastructure, as well as develop a resiliency plan that will allow it to carry out its mission effectively, if attacked. However, the necessary tools are missing that would ensure that appropriate policies, and their implementation and configurations, are being carried out correctly resulting in the minimal possibility of user errors. The need to continue to be vigilant in safeguarding sensitive and classified data and information according to their level of sensitivity and classification, and to establish and follow risk management policies, is necessary. Vigilance is needed until the cybersecurity industry can provide comprehensive solutions based on intelligent analytical models with session flows that verify their end-points in collaboration with verifiable network providers' end-to-end paths and flows.

Educating the work force continues to be important, but this will not provide a fail-safe mechanism, as insider leaks and malicious attackers are becoming sophisticated in the art of deception, phishing, and the use of hacking tools to access confidential and nonconfidential information for their own economic or political gains.

The cybersecurity industry needs to work together on the development of super-cyber-centers that automate the detection of threats, conduct assessment, and share information on potential vulnerability risks for old, existing, or new threats. In addition, alerts and updates on known attacks or confirmed exploits for critical infrastructure elements or systems must be fixed, tested, and shared to ensure key systems are protected.

CYBERSECURITY THREATS

Cybersecurity threats include cybercrime, cybervandalism, and cyberwarfare. Hence, we need to establish the appropriate classifications and terminologies regarding the types of cyberattacks and their sponsorships. These classifications and terminologies should differentiate between a state, an individual, or a group within a business, organization, or an external group of hired criminals. Regardless of how we classify a cyberattack, it has the potential to impact international relationships, businesses, economics, and political atmospheres; potentially leading to cyberbullying, cybervandalism, or even cyberwarfare amongst nations.

Despite leaps in technological advancements made in computing system hardware and software areas, we still hear about massive cyberattacks that result in enormous data losses. Cyberattacks in 2015 included: sophisticated attacks that targeted Ashley Madison, the U.S. Office of Personnel Management (OPM), the White House, and Anthem; and in 2014, cyberattacks were directed at Sony Pictures Entertainment, Home Depot, J.P. Morgan Chase, a German steel factory, a South Korean nuclear plant, eBay, and others. These attacks and many others highlight the continued vulnerability of various cyber infrastructures and the critical need for strong cyber infrastructure protection (CIP).[2]

Over the past few years, cyberattacks have targeted both industry and government organizations, but unlike those attacks, the Sony "wiper" malware attack was the first deliberate attack on a U.S. enterprise. This type of attack highlighted that state and nonstate actors are actively conducting cyber-operations to achieve a variety of political, economic, or military objectives.

Former U.S. President Barack Obama issued Executive Order 13636 in 2013 to take specific steps to improve information sharing with the private sector, raise the level of cybersecurity across our critical infrastructure, and enhance privacy and civil liberties. In

2014, the President also emphasized his "Cybersecurity Framework" to ensure:

> America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet.[3]

These efforts have increased national awareness and improved our preparedness and means both technically and legally.

Threats from a Borderless Cyberworld.

Cyberattacks have been used internationally against commercial, industrial, and Government organizations. This reflects a dangerous escalation, caused by cybercriminals or their agents, on international relations, security, and economic agreements. The potential of camouflaged cyberattacks against data systems provide state or nonstate groups and actors with a certain degree of anonymity, enabling them to cause irrevocable damage among institutions and nations.

Concerns by U.S., European Union, and Asia-Pacific officials highlight the need to standardize cybernorm laws and policies and to reduce the risks of potential cyberthreats. The U.S. Department of Defense (DoD) issued its cyber-strategy and named China and Russia as key suspects of cybercrime, which prompted both countries to deny the accusations. Subsequently, these two countries forged a cybersecurity alliance under the Shanghai Cooperation Organization (SCO), which was viewed in some circles as a response to the escalation of threats and the risk of facing preemptive steps against their cyber infrastructure.

New forms of cyberthreats continue to target government organizations and are now making their way into military institutions. These offensive actions increase the risk of cyberwarfare among nations and encourage others to carry out attacks from locations—masquerading as citizens of those locations—causing further destabilization and potential armed conflicts. If a nation prematurely takes preemptive steps or carries out a cyberattack to defend itself against perceived cyberthreats, it may inadvertently escalate a situation unnecessarily that may lead to more cyberattacks, and potentially a cyberwar or military confrontation.

Cybercrimes or cyberattacks on U.S. entities originating from within the U.S. region must be addressed by established U.S. laws and policies, but if an attacker—either state or nonstate agent—is a non-U.S. entity, then we need to adhere to the established international laws or cyber-agreements that apply.

Threats from the Bad Guys.

Cyberattacks are blurring the lines between good and bad guys. Information obtained from the recent hack of the Ashley Madison website is being used to blackmail its members or to steal their identities. Innocent people are being lured into bogus websites, which offer to reveal the identities of the Ashley Madison users, and then find themselves becoming victims when they click on targeted messages or malicious links.

The hack of an Italian surveillance cybersecurity firm called the Hacking Team, based on documents released by yet another hacking group, indicates that the Hacking Team cyber-business was for hire by anyone who was willing to pay the price, regardless of their targeted use, intended reasons for access to information, or the use of snooping tools.[4] The question of how many similar Hacking Team firms exist around the globe, and how easily a state or nonstate client can utilize their services anonymously, remains open. This revelation emphasizes the need to ensure that existing regulations and cybersecurity laws must also be extended to include laws for licensing of cybersecurity software and hacking tools developed by private cybersecurity firms, vendors, and individuals. In addition, there is even a greater need to ensure that governments adhere to international laws and agreements regarding the privacy and legality of collecting data against foreign nationals, individuals, corporations, and institutions.

Cybercriminals operate in different regions of the world and potentially can be anywhere. They may collaborate across nations and regions and take advantage of those nations where it is difficult to track them or bring them to justice because of the absence of cyberlaws. As a result, many U.S. hackers operate from outside the U.S. territories to avoid being caught and to avoid severe penalties and prison sentences. For example, a Ukrainian hacker—who was not living in the United States—was lured to travel to Turkey, where he was entrapped in order to be extradited to the United States for interrogation and to help uncover the identity of a U.S. hacker who was responsible for one of the largest retail breaches to date. The U.S. hacker was then convicted of committing fraud, breaching retail institutions, and stealing over 200 million credit card records, and received a 20-year sentence. If cyberlaws existed internationally, the capture and unraveling of the retail cyber-gang would have been much faster and it would have discouraged individuals from seeking places where the laws are weak or non-existent to commit their cybercrimes. Existence of international cyberlaws will make it easier for law enforcement agencies to coordinate against cybercriminals.

Cyberlaws and agreements amongst nations can target a cybercriminal regardless of where they are located when violating cyberlaws, and these laws can ensure a stiff penalty for the violator. Such was the case of the Israeli hacker who hacked Madonna's latest album "Rebel Heart." He pre-released some of her demo songs for monetary reasons. Coordination and collaboration amongst law enforcement agencies led to the identity and arrest of the individual, who was convicted in 2015.

Threats from the Good Guys.

It has been widely known for many years that government and law enforcement agencies have access to communication channels through lawful means such as the Communication Assistance for Law Enforcement Act (CALEA). CALEA provides the legal means or the legal framework for law enforcement agencies to access specific communication channels or tap into systems and communication networks to track, monitor, and record the targeted individual or group. Recent revelations coming from Europe and Asia-Pacific indicate there are many more state and government agencies that are requiring access to communication infrastructure, and these agencies are collecting massive amounts of data with or without lawful court orders or legal support.

Many believe that these steps are necessary to catch the bad guys; however, this may not be the case since hackers may target these channels and utilize them as avenues to access our information, thereby increasing our privacy risks and threats. The continued requests and requirements for exceptional access to infrastructure systems, as well as obtaining master keys for encrypted data communications by the U.S. Government, has raised major concerns in the technical community and the standards bodies. The technical and scientific community, led by the Institute of Electrical and Electronics Engineers (IEEE) in 2014, and more recently by a group of pioneers of Internet scientists, is worried that the damage resulting from exceptional access would be greater now than when it was provided 20 years ago.[5] This concern includes government access to systems and infrastructures through backdoors and access to encrypted data and communication channels via master encryption keys.

Threats from Terrorists' Cyberweapons and Cyberwars.

The U.S. Military is in a tough spot, having to protect the nation against enemies and adversaries across physical borders. The potential use of the virtual cyberspace by cyberterrorists and states presents a new dilemma and a potential game changer. This includes the need to deal with cyberattacks originated by rouge states, organizations, or hired help who can act as mercenaries at times of war, or from internal threats by individuals or groups armed with tools that can bring chaos. This presents an overwhelming and challenging problem for law enforcement agencies and the military, as there are many unknown factors from unknown sources that pose danger to the nation. This scenario may be summarized by stating that many amateur and professional individuals, who can access sophisticated tools, can bring havoc into critical infrastructures, thereby adding more complexity when determining who to deal with and how to respond in a lawful manner. Some of these tools could be used to launch cyberattacks anonymously, or to assume another identity in a different country and launch an attack on a government facility that may warrant swift response, thus increasing the likelihood of cyber-confrontation.

The former U.S. Secretary of Defense Ashton Carter indicated that *The Department of Defense Cyber Strategy* sets clear and specific objectives for the department to achieve over the next 5 years and beyond. In this strategy, the defense department highlights three primary cyber-missions. The first mission is that the "DoD must defend its own networks, systems, and information."[6] It states that the DoD must prepare and be ready to operate in an environment where access to cyberspace is contested. This statement clearly shows that our adversaries will consider using cyberspace to target the Internet infrastructures that will affect commercial, government, and individual entities without discrimination.

Military and law enforcement agencies also need to be vigilant on other fronts: taking on hacker groups and criminals who target their sites; defending and protecting assets, both personnel and infrastructure; and enhancing their cyber-strategies with the appropriate defenses, actions, and maneuvers. The hack into Ashley Madison's website and the subsequent release of their client list to the public is now being exploited by foreign nationals to cross-list names against hacked data from OPM and other government agencies for the purpose of blackmail and counterintelligence against U.S. Government and military personnel. This is yet another example of the need for government agencies to be vigilant and to train their employees to abide by their organization's cyber-policies.

A GOOD DEFENSE IS AN INTERNATIONAL INTELLIGENT DETERRENCE CAPABILITY

Cybersecurity is quiet challenging. The absence of cooperative efforts between technical, legal, economic, and law enforcement communities will make this challenge even more difficult to resolve. Clearly, throwing a technological solution alone at cybersecurity will not solve the problem. Similarly, establishing laws without the supporting technology for detecting, deterring, and enforcing appropriate penalties is fruitless. Therefore, there needs to be a good balance between technology and legal laws. Successful defense strategies must include establishing policies and laws and coordinating them amongst users, providers, and law enforcement communities. This will minimize cybersecurity threats to manageable risks.

The best defense is to build a good, cooperative, international, and intelligent deterrence capability based on key international cyber-norms, guidelines, and laws. This defense strategy must be enforced by standardized cybersecurity laws and practices with global support and coordination.

An independent international body is needed to oversee and address international cybercrimes, cyberattacks, cyberespionage, cybervandalism and sabotage, as well as cyberwarfare. The authors propose the establishment of an independent body called the International Cyber Union (ICU) to take legal action against international cyber-illegalities and hacks. The ICU would provide a platform for international cooperation against cybercrimes in the cyber domain.[7]

The ICU would be an independent body that could act as a partner and could coordinate through global intelligent deterrence capabilities, and would have the ability to monitor, collect, and verify international cyber-illegalities and hacks; moreover, it could take the necessary legal actions against the instigators and attackers.

THE INTERNATIONAL CYBER UNION (ICU) ORGANIZATION

The ICU as an independent organization with a structural model similar to that of the International Telecommunications Union (ITU) would promote cybersecurity research and standards. The ICU must also address the legal aspects of cybercrimes and uphold cybersecurity policies, as is being done by the International Criminal Court (ICC). However, unlike the ICC, the ICU should not require a United Nations (UN) Security Council review and vote to consider a case and/or to take action. The ICU should review cases that are generated by a Regional Cybersecurity Committee (RCC) based on a submission by a country office located within their region. All local complaints about a specific incident within a country would be submitted and considered by their Country Cybersecurity Agency (CCA). If the CCA finds reasonable evidence justifying a complaint, it would forward the complaint to the RCC, and then the RCC would determine whether to address it directly or forward it to the ICU for final judgment. The ICU would investigate and classify cybersecurity incidents and report back to the UN with factual findings. The international community would then support any action to be taken to prevent the recurrence of such incidents. These laws should be recognized and enforced globally with established cybersecurity guidelines.

The ICU, under international agreement, should have the primary responsibility for promoting international cyber-norms, peace, and security across the globe. It should be able to promote, across all member and non-member states, a set of cybersecurity norms, standard terminology, and laws. All member and non-member states would be obligated to comply with ICU decisions on matters related to international cyber-norms and cybersecurity.

The ICU would oversee all of the cyberlaws for economic, judicial, and security areas, as well as education and best practices specific to regional areas. The proposed ICU would be composed of multiple divisions, including:

1. **Policy and Administration.** This division would be mainly focused on promoting global economic and e-commerce activity, and improving cybersecurity communications amongst governments, nations, and regions within the ICU.
2. **Technical.** This division would be mainly focused on standardization of education, best practices, training, cyberattacks monitoring, tracking, mitigation, and attacker identification.
3. **Legal.** This division would be mainly focused on substantive and non-substantive legal issues, including guidelines and penalties.

The details of ICU memberships, duration, and support would be determined by the regional representatives. The leadership roles would be mainly elected and based on majority votes by representatives of member states, including world-leading economies.

The International Cyber Union (ICU) Structure.

The ICU should have a leadership role in determining and verifying whether a serious cyberattack is a threat to cyber-peace or whether it is an act of aggression carried out against a member state or a region. An individual country may file a cyber-complaint for consideration by its region, or the region may provide representation on the country's behalf to resolve the complaint. The consideration must be based on verifiable data or based on a dispute that is found to be true by the region. An individual country may also seek support of other region(s) representatives, as well as other involved countries, to settle its dispute or to reach a final settlement. The ICU should have the authority to indicate a country as a non-compliant, and it should be able to enforce the cyberlaws and sanctions or take other appropriate actions to restore global cyber-norms, peace, and security as needed. The ICU should promote collaboration and provide assistance to help protect nations or regions against cyberbullying or cyberattacks.

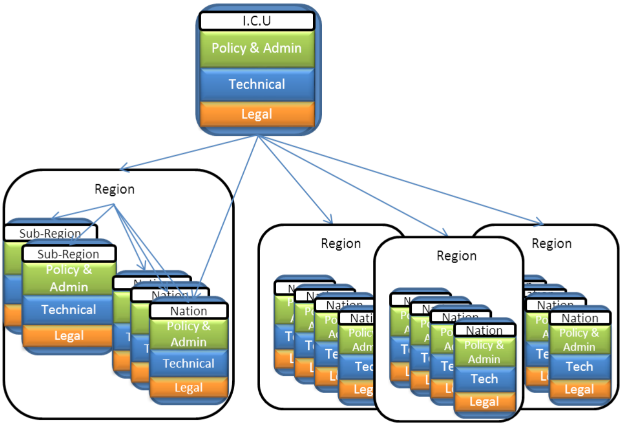


Figure 1-1. International Cyber Union (ICU) Organization Structure.

International Cyber Union (ICU) Policy and Administrative Division.

The mission of the ICU Policy and Administrative division would be to promote global economic and e-commerce activities and to improve cybersecurity communication amongst governments, nations, and regions with the ICU. In addition, this division could help to resolve cyber conflicts and foster trustful collaboration of open and secure cyber across the globe.

International Cyber Union (ICU) Technical Division.

The mission of the ICU technical division would be to promote the standardization of cyber-technology across the globe and to foster collaboration of open and secure cyber across the commercial, industrial, and educational entities. In addition, the ICU technical division could assist member states in building cybersecurity defenses, in improving their deterrent capability and technical education, and in updating their cyber infrastructure. The cyber infrastructure is mainly to improve cyberthreat detection and to access a global knowledge base of threat information.

The proposed ICU would be encouraged to collaborate with international military institutions to build and improve trust and relationships between nations and to minimize the use of cyberweapons and cyberwarfare. The ICU must also restrict the use of self-aware cyber-intelligent machines with military motives or independent cyber-intelligent systems. The use of artificial intelligence should be promoted as a good thing, especially in problem solving. However, if precautions are not taken in preventing the development of self-aware intelligent machines where humans lose control over them, then these machines could be used by attackers to cause havoc or carry out threats on infrastructures, humans, and nations.

The ICU would also be encouraged to collaborate with law enforcement agencies as well, in order to fight cybercriminals and cybercrimes. ICU technical support should include access to data based on lawful order, legal grant, or international law. Support for law enforcement access such as CALEA is expected. However, law enforcement agencies have unprecedented levels of access to communications and personal data without the need for lawful grant. In the United States, CALEA has been supported over the telephone networks since 1994, and in 2005, the Federal Communications Commission (FCC) expanded CALEA's support to Internet broadband providers, like Internet service providers (ISPs), and certain Voice over Internet Protocol (VoIP) providers. Pushing for a wholesale expansion of CALEA to all Internet communications services has been an ongoing battle in the United States since 2013, where opponents view it as an invasion of privacy, yet proponents see it as a necessary action in combating cybercrime and cyberterrorists.

In addition, many governments have added new technical requirements for backdoor access and CALEA-like interfaces of key infrastructure, such as the case in the United States. This requirement is also in response to the Snowden revelation about National Security Agency (NSA) activities. Governments that have added this requirement include the Netherlands, France, Russia, China, the United Kingdom, and many others, such as Spain, Greece, Turkey, etc. A crucial issue is that cybercriminals and hackers have discovered some of those backdoor access points that are used by law enforcement agencies. These hackers are using point-and-click wiretapping techniques that are undetectable and untraceable. This is a major hazard to cyber infrastructure and a serious risk to legitimate businesses since it is very difficult to monitor or track these cybercriminals. Furthermore, this issue is compounded by the hackers' access to encryption keys, making our privacy weaker and our encrypted storage infrastructure more vulnerable.

International Cyber Union (ICU) Legal Division.

The international community must take every measure to make the availability of cyberspace infrastructure unconditional and ensure its security. Any type of cyberattack against cyber infrastructure should be considered a cybercrime punishable by law, regardless of where the infrastructure is located. Any effort that undermines cyberspace operations should be considered a violation that must be punishable by established laws and regulations. The international community must agree that if there are any established laws at the victim's location, or the location where a cyberattack originated from, they must be applied. In the absence of such laws, default international laws should be applied instead.

The mission of the ICU legal division would be to promote cyber-policies and laws across the globe; to foster collaboration on combating cybercrimes through laws and appropriate penalties; to award punitive damages to victims of cybercrimes; and to educate members on procedural and established laws in combating cybercrimes.

The ICU legal division should be the focal point for all cyberlaws. This division would work with existing laws, whether they are substantive laws (for example, illegal access, illegal interception, data theft, and interception) or procedural laws (for example, infrastructure, data storage, and communication systems). This division would review policies, procedures, and laws and recommend selected ones for adoption to its regions, as well as to standardize those laws across all regions.

Each region may establish a regional committee as the focal point that would develop necessary laws and propose policies and procedures to: detect illegal activity, deter if possible, respond to threats, identify the criminals, seek help as necessary, prosecute the criminals, and educate its law enforcement agencies and institutions, as well as improve existing cyberlaws.

Each country may delegate an office or an individual as the focal point to oversee cybersecurity legal laws. Each country could also develop its own policies and procedures or adopt the region's approved cyberpolicies and laws. For example, legal support for law enforcement access such as CALEA, support for Open Internet, expanded CALEA support to Internet broadband providers, like ISPs and certain VoIP providers; legal support could be expanded into data traffic coming from or going to other countries.

Public policy should include open, secure, private and risk-free Internet. Individuals and organizations need to assess their need for security, determine their vulnerabilities, and decide on their acceptable levels of risk, as well as their levels of cooperation and potential investments needed to mitigate their risks. This assessment must be done without the need to worry about government backdoors and access to encryption keys, or whether these actions are violating our First Amendment rights or privacy.

INTERNATIONAL CYBER UNION (ICU) REGION AND STATE ORGANIZATIONAL STRUCTURE

International Cyber Union (ICU) Regional Organizational Structure.

Each region would be responsible for establishing each of its key divisions, such as administration, technical, and legal. The key divisions would address cyber issues related to:

1. Regional Policy and Administration:
   - Economic, E-commerce, and Social; and,
   - Government and Military Liaison to Improve Communications.
2. Regional Technical:
   - Cyber-technology and Infrastructure Improvements; and,
   - Cyber-education.
3. Regional Legal:
   - Laws Standardization; and,
   - Guidelines and Best Practices.

International Cyber Union (ICU) State Organizational Structure.

It is strongly recommended that each nation or state should have offices or coordinators that would focus primarily on cybersecurity. These should include:

1. State Cybersecurity Office. The main focus of this office would be to oversee cybersecurity activities across the state and promote agreements amongst states in its region.

2. State Cybersecurity Center. The main purpose of this center would be to coordinate nationally all activities regarding cyberspace infrastructure, security, and protection against all types of cyberthreats. National security collaboration should include local government agencies, public and private corporations, and cybersecurity firms.
3. State Cyber-Legal Office. The main goal of the Cyber-Legal office would be to review and adopt cyberlaws as recommended by the region or the ICU. Also, a nation may develop and propose its own laws for consideration by its region or other member states. This office would be responsible for all legal issues related to cyberspace, including procedures and policies to deter or to respond to inquiries, or to identify and prosecute cybercrime within its borders or in collaboration with an ICU region.

INTERNATIONAL CYBER UNION (ICU) REGIONAL MODELS

Domain Name System (DNS) Registry Model.

An important first step for an ICU in combating cybercrimes and cybercriminals is the formation of cyber-regions. These regions can take accountability for monitoring and policing traffic with established focal points that handle cybercrime activities originating and terminating in their territories. In fact, the regional Internet DNS service organizations, including: the American Registry for Internet Services (ARIN), the Latin American and Caribbean Network Information Centre (LACNIC), *Réseaux IP Européens*

(European Internet Protocol Networks [RIPE]), the Asia-Pacific Network Information Centre (APNIC), and the African Network Information Center (AFRNIC) can serve as an initial model for those regions of the world to establish RCCs.[8] For a map of the regional Internet registries, see Figure 1-2. RCCs can also establish the appropriate guidelines for improving the overall performance and security of cyberspace, as well as promote privacy and security for e-commerce activity, and affirm the need to keep governments and companies out of policing cyberspace, as taken by the FCC's consumer guide "Open Internet," which outlines their rules on keeping the Internet open.[9] Most importantly, RCC regions can function as committees that enforce, address, and resolve concerns within their region. They can also cooperate with each other on regional and global cybersecurity issues. This would form the foundation needed for an international cybersecurity body.

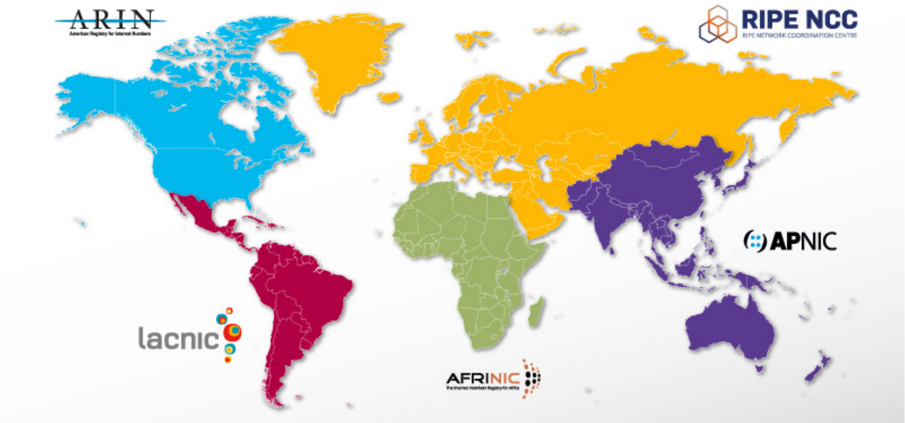


Figure 1-2. Regional Domain Name Services (DNS).[10]

Other Models.

Other models, such as the ITU, define global regions; namely Africa, the Americas, the Arab States, Asia and Pacific, the Commonwealth of Independent States (CIS), and Europe. The regional model should be simple and take into consideration the physical infrastructure that ties regions together and the traffic flow to and from a region. In addition, a region should have balanced leadership strength and the financial means required to improve infrastructure and laws.

Model considerations depend on other factors that are left to the ICU administrative leadership to determine. These include: determining whether Greenland should be part of the Americas or Europe; whether to separate North America from Central and South America or to combine them; and, whether to create a separate Arab States region or combine it with Asia. The same is true whether Australia and New Zealand form a separate region or are combined with Asia. Lastly, whether the CIS region is part of Europe or considered as a separate region.

INTERNATIONAL COOPERATION AND TRUST BUILDING

The lack of progress in overcoming cyberattacks will have a profound impact on the use of cyberspace. The potential threat of an Internet shutdown by governments is on the rise. The U.S. Government explored the notion of a kill-switch back in 2011. More recently, the Chinese Government looked at cybersecurity policies that call for a kill-switch as a measure to limit cyberattacks against their infrastructure. Hence, we need to build cooperation and trust amongst nations and to differentiate between the type of cyberattacks and the appropriate response to such attacks. E-commerce must remain open regardless of the threats faced from anywhere.

The ICU would benefit from ongoing international agreements and established laws in standardizing a minimum set of laws across the globe. This includes cybercrimes definitions, appropriate punishments, and potential penalties.

Cybersecurity agreements between the United States and other nations should continue independently in order to strengthen and build confidence in combating cybersecurity attacks and to minimize their risks across nations. Dialogues with other competitor nations are also encouraged, to improve globally the cybersecurity collaboration and to develop guidelines for combating cybercriminals and cybersecurity hackers. Consequently, it will improve the resolution of cybersecurity issues worldwide.

The ICU would also provide a platform for international cooperation in the cyber domain that ensures open cyberspace accessibility across the globe. Cybercriminals operate in different regions of the world and potentially they can be anywhere. They may collaborate across nations and regions and take advantage of nations where it is difficult to track them or bring them to justice in the absence of cyberlaws. Many U.S. hackers may operate from outside the United States to avoid being caught and potentially serving severe penalties and/or prison sentences.

It is necessary to establish rules to assess the value of these types of damages (in dollar values or the cost of replacements and reproduction) as well as defining the appropriate penalties for cyberattackers and enforcing them.

Although states, organizations, or individuals (actors) are primarily responsible for defending their information and protecting their interests from cyberattacks, they need to monitor, detect, collaborate, coordinate, and implement mitigation steps to limit their risks and damages. Those actors may opt to share information on their cyberattacks and seek help in building or improving their cyber-defenses with new capabilities. In addition, those actors are encouraged not to counter with their own cyberattacks, as these actions may provoke further attacks and may lead to even greater cyber-loss and instability.

Collaboration and cooperation with service providers will also be beneficial. Cybersecurity services offered by service providers can help against cyberattacks while they are developing newer acceptable security protection mechanisms against viruses and developing appropriate secondary defenses against data intervention and loss. This is a good step in managing and balancing an individual's roles and responsibilities with respect to cybersecurity. The service provider will work closely with industry and standards bodies to improve its real-time capability to detect, inspect, validate, and ensure that data is clean, while the user needs to focus on their education and be aware of where they click (web links). This shared security model is becoming attractive, whereby a service provider secures end-user cyber-traffic against threats for a fee. Threats such as spam, viruses, and phishing may be eliminated through service providers' intelligent networks. The end-user could then focus primarily on their cyber-education and learn how to change their typical habits of point-and-click to keep them from opening harmful email messages. These steps are key components in combating many of the threats targeting end-users.

Established Laws: Local and Regional Cyber-Norm Agreements.

The United States already has appropriate laws and guidelines regarding cybersecurity and cybercrimes. However, they are not applicable internationally. Efforts to establish international cybersecurity bodies are on the rise. For example, the European Commission established the European Cyber Crime Centre (EC3) as the focal point for handling and responding to cybercrimes. Other agreements, such as the SCO in Asia, highlight the relationships and cooperation amongst member states on key items related to information technology (IT), cyber-norms, and cybersecurity. The SCO agreement signifies the role of information and communication technology (ICT) in promoting economic and social development for the benefit of all humanity and the maintenance of international peace, security, and stability.

Intelligent Deterrence Capability.

The need to strengthen cybersecurity technologies with advanced mechanisms that help to identify where attacks originate from, and help to determine the attackers' identities, are becoming increasingly vital to ensure uninterruptible use of cyberspace.

There are many standard-setting bodies that are leading cybersecurity activities and are addressing cybersecurity concerns, such as the IEEE, Internet Engineering Task Force (IETF), and ITU. There are many computer emergency response centers such as the Computer Emergency Response Team (CERTs). Additionally, there are many regional cybersecurity consortiums, such as the Center for Infrastructure Assurance and Security (CIAS) and Cybersecurity

Research Consortium (CRC) in the United States, System Security (SysSec) in Europe, and the Indian Infosec Consortium (IIC) in Asia. There are also global and international consortiums that are addressing cybersecurity issues, such as the Consortium for Cybersecurity Action. Formed in 2012, the consortium is an effort formed by international agencies and governments to serve the international community by bringing together and promoting the most effective cybersecurity defense techniques. The ICU could further leverage the cybersecurity experiences and knowledge gained by these organizations to ensure an open and secure global cyberspace.

Information Sharing and Trust Building.

The ICU would encourage nations to cooperate with CERT centers and promote trust building amongst economic, industrial, technical, legal, government, and military institutions regarding cybersecurity threats. The ICU may utilize tools such as the ITU's Global Cybersecurity Index (GCI) to measure progress or allocate resources based on a nation or a region score (0-1) and the level of threat presented.[11] Figure 1-3 shows that the United States (dark blue) has the highest score of 0.824 out of 1. Six countries with the lowest score of zero are located in Central America, Africa, and Asia. The ITU GCI score is based on data that was collected in 2014 from nations regarding five categories: legal measures, technical measures, organizational measures, capacity building, and cooperation. The global average is about 0.28, which clearly represents non-preparedness for cybersecurity threats. Figure 1-3 also shows the GCI radar graph of the five categories that indicates that most regions in Latin America, Africa, and Asia have a GCI score below 0.5. The GCI index indicates that North America, Europe, and CIS regions are far better equipped in cybersecurity as compared to the Asia and Pacific, Arab States, the Americas (North, Central, and Latin), and African regions.

Cooperation and trust building efforts will also present additional opportunities to develop automated intelligent systems that can identify and quarantine malicious traffic flows in real-time. These intelligent systems need to fully understand the behaviors of services and their system interactions that will ultimately lead to eliminating zero-day attacks.

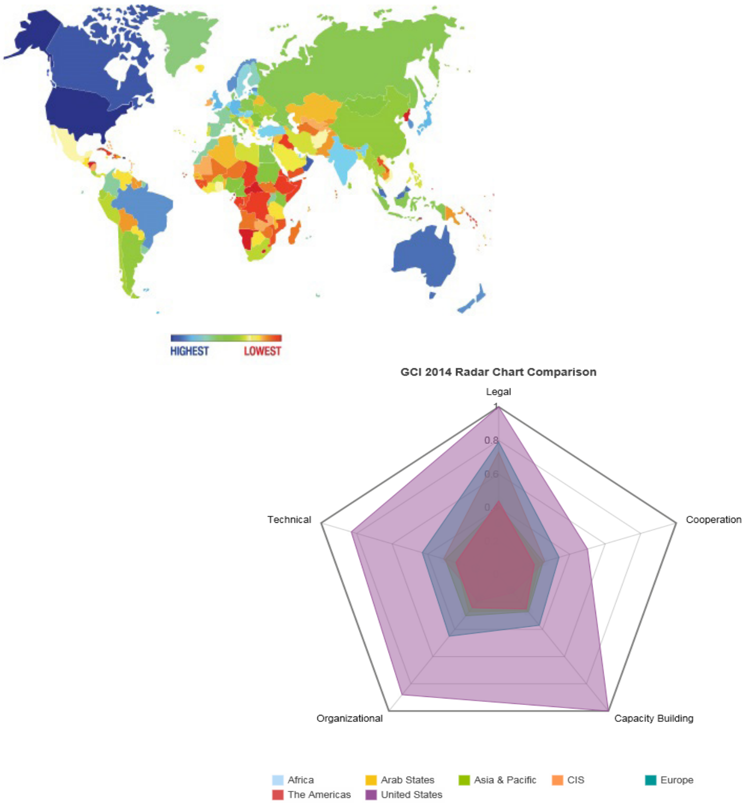


Figure 1-3. International Telecommunication Union's (ITU's) Global Cybersecurity Index (GCI).[12]

The security benefits of such systems are immense, because they provide the mechanisms to evaluate a communication flow, inspect it, and take security actions as needed. These actions can also isolate a flow, quarantine it, re-direct it to a honey pot server, study its behavior, determine its signature or if it is a zero-day attack, update the security database with relevant information, and share it with other security centers across the globe. All of these actions are done dynamically and in real-time. This model will continue to offer critical support and feedback to law enforcement agencies about the nature and behavior of an attack flow, source of the vulnerability, destination target, and method and type of attack being used.

Object-level abstraction and communication dialogue models need to be developed with cybersecurity characteristics, and control for allowing appropriate service transactions or software interactions. Models can be developed to include service parameter objects, profile(s), communication characteristics, dialogue behaviors, and signaling protocols. Such models will govern the user interaction with services via control and data layers. Change attempts are validated based on developed objects utilizing role based authentication access control to prevent any unauthorized attempt to modify public, restricted, or confidential profile characteristics, based on the user profile and authentication levels. In addition, this model will differentiate between low, medium, and high-level sensitivity and enforce high data sensitivity sessions to adhere to established policies regarding cyber-touch-points (data and control flow) based on object models associated with a user application, interface, or network.

The overall goal in securing the infrastructure is to build threat classification and taxonomy models that are primarily focused on deliberate and intentional attacks. In addition, its defense component will identify the type of threat and the required countermeasures based on the analysis of the attack. The taxonomy would include safety factors against errors such as human errors, service errors, input errors (negative testing of service features), and protocol robustness.

CONCLUSION

Recent hacks demonstrate the urgent need to create an ICU that oversees all Internet security issues internationally. The ICU should be an independent organization with a structural model that promotes cybersecurity research and standards efforts, establishes appropriate laws and their enforcements, and provides a platform for international cooperation in the cyber domain amongst its regions and member states.

The need to collaborate and develop appropriate models and predictive security solutions is becoming necessary for meaningful critical infrastructure security. Additionally, there is the need to encourage educational institutions, service providers, industry and manufacturers, user community partners, and governments to develop and utilize best of breed solutions that can accurately identify in real-time any threats being carried out across networks and to determine appropriate actions to be taken. This will also present opportunities to develop automated intelligent systems that can identify and quarantine malicious traffic flows in real-time. These intelligent systems can be developed to fully understand the behaviors of services and their system interactions that will ultimately lead to eliminating zero-day attacks.

ENDNOTES - CHAPTER 1

1. An earlier version of this chapter appeared as the paper Haidar Chamas and Tarek Saadawi, "Cyber Security: A Good Defense is a Cooperative International Intelligent Deterrence Capability," Presented at The City University of New York (CUNY), City College, Cyber Infrastructure Protection (CIP) Conference in New York on October 15, 2015.

2. Tarek Saadawi and Louis H. Jordan, Jr., eds., *Cyber Infrastructure Protection*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011; Tarek Saadawi, Louis H. Jordan Jr., and Vincent Boudreau, eds., *Cyber Infrastructure Protection: Volume II*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2013; and the present monograph.

3. "Statement by the President on the Cybersecurity Framework," The White House, Office of the Press Secretary, Washington, DC, February 12, 2014, available from *https://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework*.

4. Andy Greenberg, "Hacking Team Breach shows a Global Spying Firm Run Amok," *Wired*, July 6, 2015.

5. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner, "Keys Under Doormats: mandating insecurity by requiring government access to all data and communications," *Computer Science and Artificial Intelligence Laboratory Technical Report*, MIT-CSAIL-TR-2015-026, Cambridge, MA: Massachusetts Institute of Technology, July 6, 2015.

6. *The Department of Defense Cyber Strategy*, Washington, DC: Department of Defense, April 2015.

7. Tarek Saadawi and Haidar Chamas, "Securing Telecommunications Infrastructure against Cyber Attacks," *Georgetown Journal of International Affairs*: *International Engagement on Cyber V: Securing Critical Infrastructure*, October 2, 2015.

8. American Registry for Internet Services (ARIN), Official website, available from *https://www.arin.net/*; Latin American and Caribbean Network Information Centre (LACNIC), Official website, available from *http://www.lacnic.net/web/lacnic/inicio*; Réseaux IP Européens (European IP Networks [RIPE]), Official website, available from *https://www.ripe.net/*; Asia-Pacific Network Information Centre (APNIC), Official website, available from *https://www.apnic.net/*; African Network Information Center (AFRNIC), Official website, available from *https://www.afrinic.net/*.

9. "Open Internet," Washington, DC: Federal Communications Commission, Consumer and Governmental Affairs Bureau, available from *http://www.fcc.gov/openinternet*, last reviewed June 14, 2016.

10. Number Resource Organization (NRO), "Regional Internet Registries map," available from *https://www.nro.net/about-the-nro/regional-internet-registries*.

11. International Telecommunication Union (ITU), "Global Cybersecurity Index (GCI)," available from *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx*.

12. Figure complied from International Telecommunication Union (ITU), Global Cybersecurity Index (GCI) Interactive Map, available from *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014_charts_and_tools.aspx*; and International Telecommunication Union (ITU), Global Cybersecurity Index (GCI) 2014 Radar Chart Comparison, available from *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI_GLO_Graphics.aspx*.

CHAPTER 2

LIMITATIONS AND POSSIBILITIES OF ESTIMATING THE COSTS OF CYBERCRIME

Thomas J. Holt

INTRODUCTION[1]

Cybercrimes present a clear threat to individuals, industries, and governments alike. There are, however, substantial limitations to our understanding of both the offenders and victims of this form of crime. The lack of knowledge is due in part to an absence of quantifiable data on both the number of incidents that occur, as well as the ways that victims must remediate and repair infections and attacks. There is also minimal research considering the labor and capital costs that offenders encounter when attempting to engage in cybercrimes, as well as their potential profits. This chapter will discuss these limitations as well as explore potential models to account for offender profits using various data sources. Finally, the implications of this chapter for public policy and research are examined in depth.

LIMITATIONS AND POSSIBILITIES OF ESTIMATING THE COSTS OF CYBERCRIME

The Internet and World Wide Web have drastically changed the way businesses, governments, and citizens communicate and conduct business globally.[2] Businesses now depend on the web to solicit customers and make sales. The banking and financial services sector utilizes these technologies to provide customers with full access to accounts and electronic funds with relative ease, at all hours of the day, and from any location.[3] Home computer users can now use this technology around the clock with home-based high-speed dedicated Internet access through simple-to-use computers and mobile devices to connect to various resources.

These innovations have significant benefits, but create multiple opportunities for cybercriminals and hackers to victimize individuals and corporations alike. For example, business databases of sensitive personally identifiable information (PII) have been targeted by hackers in order to obtain bank and credit card account numbers for use in fraud and identity theft.[4] Individual computer systems are also targeted by hackers and malware users for compromise in order to establish networks of infected computers that can be leveraged for use in various cybercrime schemes.[5]

Although research on cybercrime has expanded dramatically over the last 2 decades, the focus of these studies falls into relatively uniform categories.[6] Computer science studies primarily focus on descriptive studies of the functionality and classification of attacks (or on technical solutions to identify and mitigate these threats).[7] Criminological and sociological studies tend to examine the subculture of cybercrime groups, or focus on the factors that affect the risk of victimization at the individual, or macro-level.[8]

These studies improve our knowledge of cybercrime generally, though there are still substantive gaps in our understanding of the scope and costs of cybercrime for both victims and offenders. This is due in part to the dearth of reliable and generalizable statistics on the number of cybercrimes that occur each year, as well as the extent of victimization in general population studies.[9] The majority of data sources that collect such information are largely focused on industry-specific costs and experiences, which give little insight into the experience of individual victim costs to remediate and repair infected systems or damages to financial accounts and personal financial history. Finally, there are few large-scale data sources that assess the labor and capital costs offenders incur when attempting to engage in cybercrimes, as well as their potential profits generated from various forms of cybercrime.[10]

In order to address these limitations, this chapter will examine the various existing data sources that could be used to understand offender costs, and discuss their strengths and limitations. An alternative model is presented to account for offender profits using an equation to establish profits for cybercrime based on data from web forums and marketplaces where individuals buy and sell cybercrime as a service. The limitations of this process will be considered, along with its benefits, to identify and estimate the economy of cybercrime markets. The implications of the proposed model for public policy and research will be discussed and situated in larger calls for research to improve our understanding of cybercrime generally.

CONSIDERING THE LIMITED DATA SOURCES TO EXAMINE CYBERCRIME

One of the greatest challenges to understand not only the economic impact of cybercrime, but also its prevalence and incidence, is the lack of statistics on offenses and victimization. Research on traditional forms of crime utilizes data generated from official statistics, referring to information reported by law enforcement agencies. One of the primary sources for official statistics in the United States comes from individual calls for service made to police agencies that lead to a report from an officer.[11] The Federal Bureau of Investigation (FBI) maintains an aggregated count of all crimes made known or reported to the police, and how many of those incidents were solved by arrest and published in the Uniform Crime Report (UCR). Over 90 percent of all local law enforcement agencies are included in the UCR, enabling the dissemination of the number of incidents reported to police, as well as the demographic characteristics of offenders.[12]

At present, the UCR includes data on all serious felonies, as well as a range of minor felonies and misdemeanors. The data is also historically maintained, allowing comparisons and trends of crime rates over the last few decades. There is, however, no reporting of cybercrimes made known to police or to even determine if technology was used in the completion of the offense.[13] The lack of cybercrime reporting was intentional on the part of the FBI, as they feel that the inclusion of a new offense category, or even segmentation of existing reporting categories, would negatively affect the development of historical crime trends within the United States.[14]

As an alternative, the FBI has developed an alternative data source for crime statistics called the National Incident Based Reporting System (NIBRS). This new system enables national-level reporting directly by agencies into a system that captures information on each aspect of criminal incidents reported, including whether a computer was the target of the crime.[15] The creation of NIBRS allows agencies to identify if the offender was suspected of using a computer in the course of the offense. This information provides a way to identify the total number of offenses that are facilitated in part by technology, such as fraud and child sexual exploitation.[16] However, there is no way to determine which offenses are truly cybercrimes, as there is no designation for this offense type within the NIBRS system. Furthermore, only 25 percent of all law enforcement agencies currently report data to NIBRS, which limits its utility as a measure of crimes made known to police.

Victimization studies also produce minimal information on cybercrimes. For example, the U.S. National Crime Victimization Survey (NCVS) provides a nationally representative sample of the U.S. population over the age of 16, regarding their experiences with both crime victimization and police contacts.[17] The NCVS is viewed as a primary companion to the UCR, because it provides information on criminal incidents that occurred, which may not have been reported to police, thereby providing information on the so-called dark figure of crime.

Serious violent and property crimes are captured within the NCVS data, though it provides virtually no assessment for cybercrime victimization. Recently, the NCVS has attempted to address this issue through a supplemental survey on cyberstalking victimization compared to traditional stalking.[18] There has been no measurement of more serious economic or property-motivated cybercrimes such as fraud, hacking, and malicious software use. In fact, a recent survey on identity theft victimization provided detailed statistics on financial losses suffered by victims over the age of 16 in the United States.[19] This data did not, however, provide any metrics for whether the theft was facilitated by technology or through real-world means only, limiting its application to high-tech fraud overall.[20]

The absence of useful metrics for cybercrime from official and self-reported data has led to a number of specialized reporting sources for individuals and businesses. The U.S. Internet Crime Complaint Center (IC3) has become a vital reporting mechanism for cybercrime victims. The Center was established in 2000 as a joint operation of three federal agencies: the FBI, the National White Collar Crime Center (NWC3), and the Bureau of Justice Assistance. It operates an online complaint form for cybercrime victims that asks multiple questions regarding the incident, the offenders (if known), and information on the experiences of the victim. All reports received are triaged by IC3 staff and then forwarded to an appropriate law enforcement agency when necessary.[21]

The IC3 provides one of the few individual-level sources for cybercrime victimization through an aggregated yearly report on the victimization incidents reported. This report provides details on the range of incidents reported, the age, and sex of the victim and offender, as well as the location of both the victim and the suspected or known location of the offender.[22] Victims can also report their financial losses due to victimization, though detailed breakdowns of financial harm are largely excluded from annual reports.

Though the IC3 is a unique resource, there are several limitations with the data they provide. Since victims must seek out and complete an incident report with the IC3, it is likely that their data underestimates the total number of cybercrimes taking place. In addition, the IC3 takes steps to validate all information reported by a victim, but is unable to confirm all incident details, because individuals might not have contacted law enforcement or maintained all records of their experience. Finally, the majority of complaints received involve auction fraud and non-delivery of online goods, rather than serious fraud and hacking incidents.[23] This data must be carefully contextualized before being used as a barometer for cybercrime victimization.

Though statistics on cybercrime offending and victimization rates in the general public are largely absent, there are a number of resources produced by computer security and industry sources.[24] These reports can be separated into two primary categories: 1) assessments of malware infections affecting individuals, and 2) surveys of businesses that have been affected by various forms of cybercrime.

Reports produced by antivirus vendors on the scope and costs of malware infections are particularly useful to understand the prevalence and incidence of certain tools over time. Antivirus vendors collect data on malicious software infections and publish their metrics on a quarterly and yearly basis.[25] These estimates are particularly useful to document the presence of malware in the wild at any point in time and identify trends in common attack methods. At the same time, the corporations that provide these statistics do not give much information on the way they collected the data or how representative the results may be. Typically, data is generated from machines that use their software to provide an estimate for attacks.[26] This makes it difficult to extrapolate findings to larger populations who may use different products, or no security tools whatsoever. As a result, they must be carefully evaluated for their utility in any larger estimation of the costs of cybercrime.

Those studies focusing on businesses are usually based on surveys of large businesses and organizations. One of the first such studies was developed by the Computer Security Institute (CSI), which produced a yearly report estimating the number of attacks experienced, the losses associated with the incidents, and the security strategies employed to mitigate their impact.[27] Initially, the CSI focused on the United States, but expanded to include Australia through a direct replication of their business survey. The institute published reports from 1997 to 2011, though the categories of incidents and detail provided in each report changed over time, making it difficult to develop truly historical trends.

Studies that are more recent have replicated the CSI survey model, primarily from larger organizations in the security field.[28] One of the most well cited of these studies comes from the Ponemon Institute that produces studies on the costs of various forms of cybercrime, including malware and data breaches.[29] Their study has a more global focus, as with their 2015 report on data breaches capturing 350 organizations in 11 countries around the world. Estimates from the Ponemon Institute provide some depth on the costs of cybercrime within industry, as evident in their 2015 report, which found that the average cost of a breach for a business was $3.8 million, with an average cost per record of $154. Breaches also appear to have an impact on the business future, as consumers may not come back to the organization to do business.[30]

Although this information is inherently valuable, there are several limitations within these data sets that must be noted. First, the individuals and organizations represented in the sample population change from year to year. This limits the potential for any true longitudinal assessments of trends in incidents or costs. Second, the metrics included in each report vary from year to year and reflect the shifting landscape of cybercrimes. While this may be useful to capture new trends in attacks, it limits the potential to compare certain incidents over time. This has particular salience for the Ponemon reports, as they tend to exclude large-scale incidents, such as mass data breaches, to minimize skewed data points. These incidents should not be excluded in order to more accurately reflect the landscape of victimization that occurs.

Third, the loss metrics provided are largely standardized, and they reflect averages rather than individual organizational minimums and maximums. The lack of granularity hinders the ability to understand the true costs of cybercrime within each organization. Fourth, these estimates do not reflect the costs of cybercrime to offenders or give any insights as to how attackers select their targets. Finally, the businesses and organizations sampled tend to reflect very large entities whose experiences are not generalizable to the small to medium business community.

ESTIMATING THE ECONOMICS OF CYBERCRIME

Due to the paucity of statistics and limitations in existing reporting sources, there is a need to develop models that can provide initial measurements of the costs associated with cybercrime for both victims and offenders. There is a need to identify alternative data sets that capture the scope and rate of cybercrime offending, and potential victim populations. One way to potentially measure the scope of cybercrime could be the use of open source analyses of active online communities where offenders buy, sell, and trade personal information and cybercrime services.

There is a growing literature examining the presence of illicit markets operating online, where individuals can emerge online to facilitate the sale of stolen personal information and services associated with identity crimes and hacking.[31] Spam and phishing related services are also sold, along with bulk email lists to use for spamming and email injection services to facilitate responses from victims, as are Distributed Denial of Service (DDoS) attack services and web hosting on compromised servers.[32] The majority of these studies utilize data obtained from either Internet Relay Chat (IRC) channels or web forums that can be found through search engines or other means on the open, unencrypted World Wide Web.

By understanding the processes of cybercrime markets, we can better identify their value for economic analyses of the costs of cybercrime. Specifically, markets operate through advertisements to sell or buy a specific product. Individuals post ads for others to see in a forum, website, or IRC channel after acquiring sensitive data through various means, developing malicious code, or establishing attack platforms like botnets.[33] The seller then provides a detailed explanation of their products or services, along with detail on pricing structures, preferred payment mechanisms, seller contact information, and their rules regarding transactions.[34] Some sellers will also provide information on the country of origin for personal data or where their malware is currently active, demonstrating the scope of harm caused by their activities.

Interested parties can then contact the seller, though this typically occurs through ICQ instant messaging or email messages rather than public web spaces to provide a modicum of anonymity for the participants.[35] At this point, buyers and sellers negotiate the final price for goods and services, and pay for their purchase. Most participants prefer to use electronic payment systems such as WebMoney, as they provide immediate transfers of currency and can be anonymized to some degree.[36] Cryptocurrencies, like Bitcoin, have also become popular as they are thought to be more secure than other forms of online payment.[37] Buyers must then wait for delivery of their purchase or the start of a particular service, which can vary from an immediate response to a few hours or days depending on the timeline of the vendor.

The content of advertisements for products and services provides direct information on the number of vendors active online, the quantity of products available, the nations affected, and most importantly, information on the costs for cybercrime and personal data as a service. All of these data points can be used to develop estimates of the costs of cybercrime for offenders and may provide some insights into the scope of victimization. In fact, this data could speak directly to differences in the profit margins for cybercriminals based on their technical proficiency.[38] For instance, hackers with the ability to create new software programs or gain access to sensitive databases of information may be able to garner a greater profit selling their tool to others rather than using it themselves to engage in cybercrime. Individuals who are not technically proficient could then simply purchase their services and profit from someone else's infrastructure.[39] Actors who pay for services may be able to make more money than the service provider or sellers, but face different risks from the use of services.[40] Thus, use of data from online cybercrime markets may serve as a vital source to understand the link between hacking skills and profits within the underground economy.

Despite the large body of literature that has developed around cybercrime marketplaces, few studies have provided estimates of the costs for data and services. Jason Franklin and colleagues were able to estimate the total wealth generated from an underground market found on IRC networks by examining the types and amount of products.[41] The findings demonstrated that buyers earned approximately $32 million from purchasing stolen debit and credit card information. Research by Holt and Lamkpe, and Holt and Smirnova, provided estimates for the minimum, mean, and maximum prices for data in various Russian and English-language markets that were seeking the stolen data.[42] These studies did not, however, estimate the total scope of harm caused by the markets, nor give any information on potential costs to victims.

The general lack of economic estimation may stem from the myriad complexities present in quantifying pricing, products available within these markets, and the total number of transactions completed. An individual seller may advertise various credit card types from different financial institutions across multiple nations at different overall prices.[43] Their pricing structures may change over time depending on the age of the data and the quantities available.[44] Similarly, service providers may offer discounts based on the length of time a service will be used or whether the individual is a repeat customer.[45] These factors make it difficult to disaggregate the unit price for a particular good or service in the market. Additionally, it is difficult to measure the geographic scope of harm, as sellers may not indicate the country of origin for data or services within their advertisements. Thus, there is great potential for inaccurate measures in any attempt to estimate buyer profits and the potential scope of harm caused to a given nation.

Measuring prices are also complicated by the fact that the negotiation process between buyers and sellers occurs privately. The hidden nature of the transactions makes it exceedingly difficult to determine the final unit price for information or a service. Furthermore, the quantities purchased in any transaction cannot be determined, as well as the effect of bulk purchasing on the final negotiated price for data.[46]

Despite these limitations, there may be value in using an alternative measure derived from the feedback and reviews provided by data buyers in these markets. Since transactions take place in private, customers in cybercrime markets are encouraged and expected to post their experiences with a seller publicly on their thread in forums to describe their encounters.[47] This public display of feedback provides information on the practices of sellers and the ability of potential customers to trust vendors. If a customer did not feel satisfied, either because the goods were not as advertised or were undelivered, they can post their experience on the seller's thread. This sort of negative feedback provides a visible sign that a vendor is untrustworthy. In much the same way, those who were pleased by their interactions could make a post about the seller's practices or data.[48]

The use of feedback provides a proxy measure for the number of transactions completed within a given thread in a forum. Both positive and negative feedback demonstrate successful transactions in favor of sellers, as they obtain funds from buyers regardless of whether or not the data or services purchased worked. Since buyers expect to turn a profit from their purchase, they depend on working account information in order to maximize their return on investment. Positive feedback acts as a proxy measure indicating that a buyer was able to use the data purchased or apply the services for which they paid. Should an individual not receive the data or service they purchased, or if it either consists of inactive accounts, false information, or is of poor quality, they have no legal recourse to offset their losses.[49] Negative feedback indicates that a buyer was unable to utilize the goods and services they purchased.

Feedback can be quantified as a means to understand how many transactions may have occurred and the secondary profits that buyers can generate from successful applications of the information or service purchased. There is a need to identify the conditioning factors that may affect the profits made by individuals purchasing data or services within these markets. There is no guarantee that all accounts purchased from a data seller will be active and valid at the time of purchase.[50] In much the same way, cybercrime services may also fail depending on the technical skills of the buyer and the infrastructure of the seller.[51] Financial institutions may also be able to increasingly alert customers if their information may have been lost through a breach and reissue cards to reduce the ability of criminals to use the information.[52] Similarly, antivirus vendors and security products may keep DDoS attacks and other hacking services from being successfully applied by attackers against a target.[53] As a result, there is no way for a buyer to know what their proportion of success will be from any transaction regardless of the vendors' intent.

In all, there are multiple challenges inherent in documenting the scope and economy of cybercrime using data from primary sources. At the same time, there is sufficient information present in order to generate preliminary—though very limited—models and estimates for the revenues generated by buyers and sellers in online black markets. Such estimates are an extremely valuable first step in the process of estimating the money made by cybercriminals who serve as primary hackers and those who simply pay for their tools.

MODELING CYBERCRIME SERVICE AND DATA VENDORS' REVENUES

Based on the available data points provided within cybercrime forums, it might be possible to estimate the potential profits vendors may earn using the following formula:

Total Sellers' Revenues = total feedback × lot size × advertised price × probability of success

Specifically, negative and positive feedback can be totaled from each thread within each vendor's advertisement to assess the total number of sales completed.[54] Feedback may include information about either transactions that did not occur (fraudulent posts) or situations where buyers and sellers were not able to get 100 percent of revenue from the transaction. In both situations, the seller would still have earned money from these exchanges, making this a reasonable way to estimate revenues.

Additionally, products and services within cybercrime markets are offered at an individual unit price, such as a per hour rate of attacks or the price per credit or debit card.[55] Customers are encouraged to purchase products in large quantities or lots that are varied in size based on vendors and product types. For instance, sellers offering credit and debit card data historically prefer buyers to purchase data in quantities of 100 or more accounts at a time.[56] Malware vendors typically sell their code as an individual item, while DDoS vendors prefer that customers use their service over a 24-hour period.[57]

Economic models of profit must therefore condition the quantity of data sold per lot to more accurately capture the prospective revenue of sellers. The transactions may have various sizes of lots, starting with 25 and increasing to 100 accounts. Seller profits are estimated based on the observed number of transactions (e.g., 585 for dumps in forums), multiplied by the number of potential lot-sizes, multiplied by the price per item (ranging from minimum to maximum prices).

To calculate seller profits from all sales, the posted prices in an ad can be used to generate measures for the minimum, maximum, mean, and median advertised price. There is a prospective range for data and services, and all four figures may provide estimates that are more accurate for the potential range of revenues generated by sellers.[58] These figures can also be standardized from the preferred currencies of vendors into a single type, which is most commonly U.S. dollars (USD).[59]

A final factor that must be included is the fact that not every transaction may lead to feedback for the seller. A buyer may choose not to provide feedback so as to minimize their online presence and hide their overt involvement in cybercrime markets. Others may simply opt not to participate in the collegial nature of the marketplace.[60] Some feedback may also be falsified in order to increase the perceived reliability of a vendor in the market. An unscrupulous seller may create multiple user profiles and post fictitious reviews indicating that they successfully completed a transaction in order to drive real customers to the vendor.[61]

To control for the possibility of measurement error based on false or missing feedback, it is necessary to control for the probability of actual transactions completed. Since it is impossible to know the accuracy of feedback provided, an alternative solution would be to condition the outcomes by quartiles in order to provide estimates for situations where feedback does not represent correct transactions due to various factors to avoid overestimation. For instance, the use of a 25 percent increment is intended to reflect seller profits in the event that the majority of feedback posted was faked. Each incremental increase demonstrates the increased profit margins for a seller; up to 100 percent accuracy where all feedback received is assumed correct. Up to 125 to 200 percent would overestimate the potential feedback received and lead to greater overall profits for the seller.

MODELING CYBERCRIME AND DATA BUYERS' REVENUES

A similar formula can be used to assess the revenues generated by participants within cybercrime markets utilizing elements observed within the exchanges in any thread. To calculate buyers' profits, the following formula can be used:

$$\text{Total Buyer Profits} = (\text{positive feedback} \times \text{lot size} \times \text{average loss for identity theft} \times \text{probability of success}) - \text{advertised price of data}$$

First, the number of successful transactions for buyers' revenues should be calculated using only positive comments posted by forum participants, because they signal an individual was able to utilize any of the data they purchased. This information provides a more accurate potential estimate for buyer earnings, as negative feedback should be an indication of a failed or unsuccessful exchange. The size of the lot of data or services should also be accounted for in order to utilize a similar basis for the total number of accounts purchased.

There is, however, a complication involved in the assessment of prospective buyer profits based on the type of cybercrime being examined. In the event an individual purchases credit or debit card data, then loss estimates could be acquired from official data sources, such as the U.S. Bureau of Justice Statistics or the United Kingdom (UK) National Fraud Authority (NFA) Annual Fraud Indicator loss estimates. These are some of the only useful figures available to identify the losses suffered by individuals on the basis of identity theft or fraud victimization year to year. The figures published by these agencies, however, do not disaggregate high- and low-tech identity theft. These data sources may skew the actual profits, as it may be that high-tech identity fraud is less frequent compared to traditional means, such as acquiring personal information via robbery. At the same time, they provide a more accurate reflection of victim costs than other sources, such as the Ponemon Institute and other industry sources that report on business losses. Thus, victim-based estimates from population surveys should provide the most accurate estimates for potential profits for cybercriminals.

In order to control for the potential for data that may not be useable, quartile measures could again be used to capture potential buyer revenues. Since it is unlikely that all data purchased from a seller may be active, the use of quartiles provides a way to represent the adjusted profits of a buyer based on useful data.

Multiplying transactions by 25 to 100 percent can reflect the potential profits of a data buyer in the event that a portion of the data could be used to engage in fraud.

Finally, the advertised price for stolen data must be subtracted from this amount to serve as a proxy for buyers' costs. This figure does not provide any measures for the costs of labor and other components of buyers' expenditures, nor does it capture any variations in the final negotiated price paid for a good or service. At the same time, the cost figure can be generated from publicly posted information and used as a means to capture the various costs they may incur.

DISCUSSIONS AND CONCLUSIONS

Though cybercrime poses a clear and persistent threat to individuals, industries, and governments, there is little generalizable information available to understand its scope, nor the economic impact these offenses have on victims. Researchers have called for improved measures of cybercrime in both official and self-reporting data sources for the last 15 years.[62] There has been incremental progress in law enforcement data sources, though they are still largely insufficient to understand cybercrimes such as hacking and malware infections. Industry sources provide an alternative data source, but they are difficult to generalize to the entire population of Internet users. Others are focused on business losses, which do not afford insights into individual losses from victimization, costs incurred by offenders, or the revenues cybercriminals may generate from various schemes.

To address these shortcomings, this chapter argues for the development of primary data from cybercrime markets operating online to estimate the economic gains made by buyers and sellers of services.[63] Information is posted in clear text via advertisements posted in forums and websites, which allows researchers to quantify pricing structures for various data and services. The use of customer feedback also allows researchers to estimate the number of transactions performed between buyers and sellers, and differentiate between successful and failed transactions through the use of positive or negative comments from buyers. It may be possible, using this information, to develop metrics for the price paid for data and services, as well as the prospective revenues that could be generated by sellers and buyers.

The formula presented to estimate buyer and seller profits is exploratory in nature and may have utility to understand the range of revenues generated by buyers and sellers separately. This model is also limited by several factors, which must be considered before implementation by researchers. First, a vendor who received no feedback in observed threads would be excluded from this analysis, though they may have had buyers for their products. If they had recently posted an ad, or had minimal customer interest in their products, any transaction that may have been completed but not commented on would go uncounted. Thus, researchers must carefully consider how to develop samples of threads from cybercrime forums in order to better reflect the economy within that market.

Second, this model focuses only on vendor and buyer profits. These estimates do not provide any estimates for the total losses suffered by victims, including retailers or card processors. In addition, this figure does not include labor costs on the part of cybercrime vendors or buyers. It is unknown how many man-hours are necessary to maintain a botnet, develop spam lists, or engage in a successful data breach to acquire economic information. The lack of estimates on criminal costs is due not only to the difficulty researchers have in developing qualitative data to address these questions, but also to the range of skill and technical expertise evident in hackers and cybercriminals relative to the complexity of the attack vector and target security.[64] In addition, the equation presented does not factor in the need for ancillary services to support a cybercrime scheme, such as web-hosting or the use of money laundering services.[65] The estimates of this equation, however, can serve as a valuable baseline to assess the initial size of the economy based on direct exchanges between buyers and sellers.

Third, this equation would present ranges for the profits generated by cybercriminals, which does not give substantial clarity on the actual economy of this market. This is due in part to the fact that the advertised price for data may not capture the true amount an individual pays for data or services, since transactions take place outside of the forums.[66] The only way to acquire such information would be to capture the personal exchanges between participants in the markets, or engage in covert transactions with prospective sellers, which creates ethical challenges. Increased clarity in reporting is vital to move criminological research beyond speculation and case studies into quantifiable areas of loss calculation. In turn, we can better understand the economic impact of stolen data markets for individual victims.

ENDNOTES - CHAPTER 2

1. An earlier version of this chapter appeared as the paper Thomas J. Holt, "Limitations and Possibilities of Estimating the Costs of Cybercrime," Presented at The City University of New York (CUNY), City College, Cyber Infrastructure Protection (CIP) Conference in New York on October 15, 2015.

2. Graeme R. Newman and Ronald V. Clarke, *Superhighway Robbery: Preventing E-commerce Crime*, Cullompton, UK: Willan Press, 2003; David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge, UK: Polity Press, 2007.

3. Newman and Clarke; Wall; Lance James, *Phishing Exposed*, Rockland, MA: Syngress Publishing Incorporated, 2005.

4. Jason Franklin, Vern Paxson, Adrian Perrig, and Stefan Savage, "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants," in Peng Ning, gen. chair, and Sabrina De Capitani di Vimercati and Paul Syverson, pro. chairs, *Proceedings of the 14th ACM conference on Computer and communications security 2007 Alexandria, VA, USA – October 29 - November 02, 2007*, New York: Association for Computing Machinery, 2007, pp. 375-388; Thomas J. Holt and Eric Lampke, "Exploring stolen data markets online: products and market forces," *Criminal Justice Studies*, Vol. 23, Iss. 1, 2010, pp. 33-50; Kimberly Peretti, "Data Breaches: What the Underground World of 'Carding' Reveals," *Santa Clara High Technology Law Journal*, Vol. 25, Iss. 2, 2009, pp. 375-413.

5. Paul Bächer, Thorsten Holz, Markus Kötter, and Georg Wicherski, "Know your Enemy: Tracking Botnets: Using honeynets to learn more about Bots," The Honeynet Project and Research Alliance, 2005, updated August 10, 2008, available from *www.honeynet.org/papers/bots/*; Adam M. Bossler and Thomas J. Holt, "On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory," *International Journal of Cyber Criminology*, Vol. 3, Iss. 1, June 2009, pp. 400-420; Thomas J. Holt, "Exploring the social organisation and structure of stolen data markets," *Global Crime*, Vol. 14, Iss. 2-3, 2013, pp. 155-174; Jose Nazario, *Defense and Detection Strategies against Internet Worms*, Norwood, MA: Artech House Incorporated, 2003.

[6] Thomas J. Holt and Adam M. Bossler, "An Assessment of the Current State of Cybercrime Scholarship," *Deviant Behavior*, Vol. 35, Iss. 1, 2014, pp. 20-40.

[7] Nazario; Jason D. Collins, Vincenzo A. Sainato, and David N. Khey, "Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors," *International Journal of Cyber Criminology*, Vol. 5, Iss. 1, 2011, pp. 794-810; Sameer Hinduja and Brandon Kooi, "Curtailing cyber and information security vulnerabilities through situational crime prevention," *Security Journal*, Vol. 26, Iss. 4, October 2013, pp. 383-402.

[8] For an examination of the subculture of cybercrime groups, see Holt, "Exploring the social organisation and structure of stolen data markets"; Thomas J. Holt, "subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures," *Deviant Behavior*, Vol. 28, Iss. 2, 2007, pp. 171-198; Alice Hutchings and Thomas J. Holt, "A Crime Script Analysis of the Online Stolen Data Market," *British Journal of Criminology,* Vol. 55, Iss. 3, 2015, pp. 596-614. For factors that affect the risk of victimization at the individual level, see Bossler and Holt, "On-line Activities, Guardianship, and Malware Infection"; Fawn T. Ngo and Raymond Paternoster, "Cybercrime Victimization: An examination of Individual and Situation level factors," *International Journal of Cyber Criminology*, Vol. 5, Iss. 1, January-July 2011, pp. 773-793. For macro-level, see Alex Kigerl, "Routine Activity Theory and the Determinants of High Cybercrime Countries," *Social Science Computer Review,* Vol. 30, Iss. 4, 2012, pp. 470-486.

[9] Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, New York: Oxford University Press, 2009; Thomas J. Holt and Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*, London, UK: Routledge Press, 2016.

[10] Holt and Bossler, *Cybercrime in Progress*.

[11] Federal Bureau of Investigation (FBI), *Uniform Crime Reporting Handbook*, Washington, DC: U.S. Department of Justice, 2004.

[12] *Ibid*.

13. Maria Tcherni, Andrew Davies, Giza Lopes, and Alan Lizotte, "The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?" *Justice Quarterly*, Vol. 33, Iss. 5, 2016, pp. 890-911.

14. Federal Bureau of Investigation (FBI), *National Incident-Based Reporting System: Volume 1: Data Collection Guidelines*, Washington, DC: U.S. Department of Justice, 2000.

15. *Ibid*.

16. *Ibid*.

17. Shannon Catalano, *Stalking victims in the United States-Revised*, Washington, DC: U.S. Department of Justice, 2012.

18. *Ibid*.; Matt R. Nobles, Bradford W. Reyns, Kathleen A. Fox, and Bonnie S. Fisher, "Protection against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization Among a National Sample," *Justice Quarterly*, Vol. 31, Iss. 6, 2014, pp. 986-1014.

19. Erika Harrell and Lynn Langton, *Victims of identity theft, 2012,* Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, 2013.

20. *Ibid*.

21. Internet Crime Complaint Center (IC3), *2014 Internet Crime Report,* Washington, DC: Internet Crime Complaint Center, Federal Bureau of Investigation, 2015, available from *https://www.ic3.gov/media/annualreport/2014_IC3Report.pdf*.

22. *Ibid*.

23. *Ibid*.

24. Computer Security Institute (CSI), *2010/2011 Computer Crime and Security Survey*, New York: Computer Security Institute, 2011; Ponemon Institute, *2014 Cost of cybercrime study: United Kingdom,* Traverse City, MI: Ponemon Institute, 2015; Symantec Corporation, *Symantec Internet Security Threat Report: 2014*, Vol.

19, 2013 Trends, Mountain View, CA: Symantec Corporation, 2014, available from *https://www.symantec.com/content/dam/symantec/docs/security-center/archives/istr-14-april-volume-19-en.pdf*.

25. Symantec Corporation; McAfee and the Center for Strategic and International Studies (CSIS), *Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II*, Washington, DC: McAfee and Center for Strategic and International Studies, June 2014.

26. Symantec Corporation.

27. CSI.

28. Ponemon Institute.

29. *Ibid*.

30. *Ibid*.

31. Franklin *et al*.; Holt and Lampke; Holt, "Exploring the social organisation and structure of stolen data markets"; Hutchings and Holt; Cormac Herley and Dinei Florêncio, "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy," in Tyler Moore, David J. Pym, and Christos Ioannidis, eds., *Economics of Information Security and Privacy*, New York: Springer, 2010, pp. 33-53; Thomas J. Holt, Yi-Ting Chua, and Olga Smirnova, "An exploration of the factors affecting the advertised price for stolen data," in *eCrime Researchers Summit 2013 (eCRS 2013)*, Proceeding of the 2013 APWG eCrime Researchers Summit, eCRS 2013, San Francisco, CA, September 17-18, 2013, Institute of Electrical and Electronics Engineers (IEEE) Computer Society, 2013, pp. 1-10; Marti Motoyama, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker, "An Analysis of Underground Forums," in *Proceedings of the 2011 ACM SIGCOMM conference Internet Measurement Conference (IMC'11)*, Berlin, Germany, November 2-4, 2011, New York: AMC Publications, 2011, pp. 71-79; Frank Wehinger, "The dark net: Self-regulation dynamics of illegal online markets for identities and related services," in Nasrullah Memon and Daniel Zeng, eds., *2011 European Intelligence and Security Informatics Conference EISIC 2011: 12-14 September 2011, Athens, Greece*, Los Alamitos,

CA: Institute of Electrical and Electronics Engineers (IEEE) Computer Society, Conference Publishing Services, 2011, pp. 209–213; Michael Yip, Craig Webber, and Nigel Shadbolt, “Trust among cybercriminals? Carding forums, uncertainty, and implications for policing,” *Policing and Society*, Vol. 23, No. 4, 2013, pp. 1-24.

32. Franklin *et al*.; Motoyama *et al*.; Bill Chu, Thomas J. Holt, and Gail. J. Ahn, *Examining the Creation, Distribution, and Function of Malware On-Line*, Technical Report for National Institute of Justice, NIJ Grant No. 2007-IJ-CX-0018, Washington, DC: National Institute of Justice, 2010.

33. Franklin *et al*.; Holt, “Exploring the social organisation and structure of stolen data markets.”

34. Franklin *et al*.; Holt and Lampke; Holt, “Exploring the social organisation and structure of stolen data markets”; Hutchings and Holt.

35. Franklin *et al*.; Holt and Lampke; Holt, “Exploring the social organisation and structure of stolen data markets”; Hutchings and Holt.

36. Wehinger.

37. Monica J. Barratt, “SILK ROAD: EBAY FOR DRUGS,” *Addiction*, Vol. 107, Iss. 3, March 2012, pp. 683-684.

38. Thomas J. Holt and Max Kilger, “Know Your Enemy: The Social Dynamics of Hacking,” *Know Your Enemy Series White Paper*, The Honeynet Project, May 29, 2012, available from *https://honeynet.org/papers/socialdynamics*.

39. Holt, “Exploring the social organisation and structure of stolen data markets.”

40. *Ibid*.; Hutchings and Holt.

41. Franklin *et al*.

42. Holt and Lampke; Thomas J. Holt and Olga Smirnova, *Examining the Structure, Organization, and Processes of the Interna-*

tional Market for Stolen Data, Washington, DC: U.S. Department of Justice, 2014.

43. Franklin *et al*.; Holt and Lampke; Herley and Florêncio.

44. *Ibid*.

45. Holt, "Exploring the social organisation and structure of stolen data markets."

46. Franklin *et al*.; Holt and Lampke; Herley and Florêncio; Motoyama *et al*.; Wehinger.

47. Holt and Lampke; Motoyama *et al*.

48. Holt and Lampke; Holt, "Exploring the social organisation and structure of stolen data markets"; Hutchings and Holt; Motoyama *et al*.

49. Holt and Lampke; Holt, "Exploring the social organisation and structure of stolen data markets."

50. Franklin *et al*.; Holt and Lampke; Hutchings and Holt.

51. Holt, "Exploring the social organisation and structure of stolen data markets."

52. Newman and Clarke; Peretti; Tara Seals, "2014 So Far: The Year of the Data Breach," *Infosecurity Magazine*, August 12, 2014, available from *www.infosecurity-magazine.com/news/2014-the-year-of-the-data-breach/*.

53. Symantec Corporation.

54. Holt and Lampke; Holt, "Exploring the social organisation and structure of stolen data markets"; Motoyama *et al*.

55. Franklin *et al*.; Holt and Lampke; Holt, "Exploring the social organisation and structure of stolen data markets"; Motoyama *et al*.

56. Franklin *et al*.; Holt and Lampke; Herley and Florêncio.

57. Holt and Lampke; Chu, Holt, and Ahn.

58. Holt and Lampke; Holt and Smirnova.

59. Franklin *et al*.; Holt and Lampke; Holt, "Exploring the social organisation and structure of stolen data markets"; Motoyama *et al*.; Yip, Webber, and Shadbolt; Holt and Smirnova.

60. Holt, "Exploring the social organisation and structure of stolen data markets"; Chu, Holt, and Ahn.

61. Hutchings and Holt.

62. Wall; Holt and Bossler, "An Assessment of the Current State of Cybercrime Scholarship"; Brenner.

63. Franklin *et al*.; Holt and Lampke; Holt, "Exploring the social organisation and structure of stolen data markets"; Motoyama *et al*.

64. Holt and Kilger.

65. Holt and Lampke.

66. Franklin *et al*.; Holt and Lampke; Hutchings and Holt; Motoyama *et al*.; Wehinger; Yip, Webber, and Shadbolt.

CHAPTER 3

MALICIOUS SPAM: THE IMPACT OF PROSECUTING SPAMMERS ON FRAUD AND MALWARE CONTAINED IN EMAIL SPAM

Alex Kigerl

INTRODUCTION[1]

Spam has grown in parallel with the Internet. Spam can be more than just a nuisance; it can also be fraudulent and malicious. Spam is one of the most common attack vectors for perpetrators of fraud and distributors of malware. The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN SPAM Act) is U.S. federal legislation that was passed in response to the growing spam problem. Current research suggests that prosecutions under the CAN SPAM Act appear to reduce overall spam volume, as well as increase certain types of spam law compliance. However, it is uncertain to what degree of impact the CAN SPAM Act might have had on more serious forms of cybercrime contained in spam, such as malware and fraud. The present research sought to address this question by assessing the impact that prosecutions of spammers has had on a sample of 5,490,905 spam emails sent between 1998 and 2013. Machine learning and data mining techniques were used to build one measure of fraud and two measures of malware distribution contained in the spam sample. Findings suggest little impact of the CAN SPAM Act on fraud, but a possible deterrent impact on malware. More damages judged against spammers and more arrests of spammers appear to be associated with fewer malicious links contained in spam. It is suggested that future research should look at prosecutions of offenders committing fraud and malware distribution directly to further examine these effects.

MALICIOUS SPAM: THE IMPACT OF PROSECUTING SPAMMERS ON FRAUD AND MALWARE CONTAINED IN EMAIL SPAM

Email spam has grown with the parallel growth in technology and Internet connectivity worldwide.[2] Spam can be more than just bothersome email marketing; it can also facilitate fraud and malware distribution. The harmful nature of this spam is why legal responses to such growing crimes ought to be effective. Forms of cybercrime not facilitated by email spam, such as hacking and cyberattacks on businesses, have been found to be reduced with increased prosecutions and incarcerations of such offenders mentioned in news reports.[3] However, email spam is often a primary means to facilitate such crimes.

Email spam itself is also a form of cybercrime in the United States, regulated by the CAN SPAM Act.[4] The CAN SPAM Act does not illegalize the sending of spam, but instead regulates the methods on how it is composed and sent. The Act has been associated with reductions in the amount of spam sent, as well as spammer compliance with the Act on some measures.[5] However, it is uncertain to what extent the Act might have had an impact on more serious forms of cybercrime, such as malware and fraud. The Act does not regulate such crimes, but instead regulates the sending of commercial spam messages themselves. However, spam is one of the predominant methods for facilitating both fraud and malware online. It is questioned whether the Act has also had an impact on these forms of crime.

This chapter seeks to answer this question by analyzing a time series dataset of spam received within the United States between 1998 and 2013. The study incorporates measures of CAN SPAM Act prosecution activity (fines, arrests, convictions, etc.), as well as multiple economic, technological, and demographic related controls. Equipped with these techniques, the extent to which regulations of electronic spam can affect more serious cybercrimes facilitated by email spam can be identified.

THE STATE OF FRAUD AND MALWARE TODAY, AND WHY RESEARCH IS NEEDED

Email spam has experienced a growth since its inception and today makes up 72 percent of all emails sent worldwide. Over half of all Internet traffic in general, not just email traffic, is actually spam.[6] Email spam is not the only type of spam that can be sent; it can take any form where electronic communications exist, such as text messaging, chat, and search engine spam. However, email spam is the most prevalent form of spam.[7] Loss of human resources due to the nuisance of spam was estimated to be at $22 billion in 2004.

Spam can be harmful beyond just being a nuisance. Most spam today is sent from a type of malware called a botnet. As much as 76 percent of all spam is sent from such botnets.[8] A botnet is a network or cluster of malware-infected machines that the cybercriminal can control remotely over the Internet. The victim that owns the infected computer is unaware of the botnet installation, and so the botnet master can use as many as thousands of remote PCs running in parallel to flood user inboxes with spam. The number of Internet-connected computers that are infected with at least one botnet is estimated to be at 14 percent.[9]

Spam is not only sent from malware, but is also often used to distribute malware. Among spam messages that provide a link to the recipient, 25 percent of them link to malware. Of the websites that spam messages linked to, 67 percent were considered to be legitimate websites that had been compromised by hackers. Trend Micro reported that 25 percent of malicious Uniform Resource Locators (URLs) were hosted on servers located within the United States in the 2nd quarter of 2014.[10] All other countries were just 3 percent of hosted malware or less. Among the victims of malware, 36 percent resulted in financial losses.[11] An attacker might steal all of a victim's savings with a single successful attack on an e-payment or e-banking account. Businesses lose an estimated $6,500 per hour to recover from a DDoS attack and as much as $3,000 a day to recover from a malware attack.[12]

The technical ability to write malicious code is not necessary to profit from cybercrime. Many times an attacker does not have to exploit a technical vulnerability in a computer system to perpetrate his or her schemes. Often the weakest link is the human target itself, as it is easier to socially engineer a human victim than it is to engineer the breach of a security flaw. That is why there were 262,813 complaints of Internet fraud in 2013, according to the Internet Crime Complaint Center in the United States.[13]

There are two common forms of Internet fraud most often perpetrated using email spam. The first is phishing, whereby an attacker attempts to acquire a victim's "credential goods" through deceit. A credential good is any information a person may have that can be converted into cash, such as credit card numbers, Internet banking logins, or social network member passwords. Typically the phisher will link the victim to a website that looks identical to a trusted source the victim uses, such as a bank, whereby the user is requested to fill out a web form to capture the sought after credential goods.

The United States is targeted the most by phishing attacks, suffering 60 percent of worldwide phishing volumes.[14] In 2013, phishing was up 160 percent since 2011, costing an estimated $5.9 billion in losses worldwide. When an individual falls victim to a phishing attack, the average amount lost is $1,800.[15] However, businesses are often targeted, which result in a loss of $20,070 per business if successful.[16]

The second form of Internet fraud is the advance fee fraud scheme, also known as 419 scams. These methods rely on even fewer technical skills to pull it off, as the scheme is entirely that of social engineering. Advance fee fraud is a confidence trick, whereby the fraudster contacts the victim via spam email with some sort of proposal. The proposal can be anything the victim wants, such as news of lottery winnings, a profitable business deal, or romantic relationship over an online dating website. However, before the deal can be finalized, the victim must wire the fraudster an "advance fee." Of course, there is no deal that the fraudster will deliver, and the scammer will continue to string the victim along, making additional advance fees for as long as possible.

Because the fraudster can continue to victimize the same person many times before it is realized to be a scam, losses due to advance fee fraud can be greater than that of a phishing attack. Small losses are considered to be $200 to $30,000 per victim over the course of half a year.[17] Higher losses can reach as much as $210,000 over a period of 1 1/2 years.

The loss of money is not the only risk that advance fee fraud imposes. In some cases, victims are lured to the home countries of the fraudster as part of the scheme, such as Nigeria where these scams are highly prevalent. If successful, the victim is kidnapped and held ransom for more money. Between 1996 and 2013, there were a total of 31 murders, 35 suicides, 49 kidnapping and hostage situations, and 1,512 bankruptcies due to advance fee fraud. Kidnappings as part of advance fee fraud are only growing, as more people become aware of fraud over the Internet, and so fraudsters must resort to more drastic measures to continue making the same amounts of money.[18]

THE CAN SPAM ACT

The laws against spam that are of interest to this research are those included under the U.S. CAN SPAM Act of 2003. The legislation was passed by Congress in 2003, going into effect on January 1, 2004. The regulations inherent in the bill set requirements that electronic commercial messages must adhere to when sending advertisements to recipients electronically (including email and other electronic means of communication). The bill does not prohibit unsolicited commercial emails, but rather it regulates the way they are sent and the content that is delivered. The messages must be truthful and not fraudulent. The sender must also comply with a recipient's express request to opt-out of all future emails.

One of the first and basic rules set forth in the Act forbids the falsification of email headers. The headers of an email message include the recipient's address, the sender's address, the return or bounce address, and additional routing details contained in the headers. Spammers will often fabricate false header details. Another header field in an email that is subject to restriction is the subject header. Senders are not permitted to write header titles intended to mislead the recipient on what the contents of the message body are before opening the email. Subject headings must relate to the contents of the email.

The sender must provide a channel for the recipient to opt-out of further advertisements. Opt-out is the ability of the recipient to make a request to discontinue receiving spam and the willingness of the spammer to honor those opt-out requests. The spammer is not required by law to get opt-in from the recipient. The sender's valid physical postal address must also be included somewhere in the body of the email, or at least an address where to contact the sender. Lastly, the message contents or subject heading must identify itself as an advertisement. Providing this notice can help the intended recipient decide if they want to read or continue reading the email when sorting mail.

THE CAN SPAM ACT AND DETERRENCE THEORY

Deterrence is defined as the omission of an act as a response to the perceived risk and fear of punishment for contrary behavior.[19] In the context of the CAN SPAM Act, the penalties under the Act are intended to serve as such a deterrent effect. A punishment does not have to prevent an offense entirely in order to be effective.[20] A punishment can simply reduce the approximate severity of the offense itself.

Termed “partial deterrence,” if an offender commits an offense lower in severity due to an expected threat of punishment, this is also considered to be a deterrent effect. While likely not profitable enough for the typical spammer to comply with all the provisions of the CAN SPAM Act, he or she might avoid committing some aggravations of the Act, or reduce the number of violations contained in each spammed message, such as routing spam messages through a botnet.

Prosecutions of spammers may also serve as a stronger deterrent of less serious offenders, while more serious cybercriminals utilizing email spam will continue offending. A serious offender is already taking larger risks when choosing to engage in cybercrime, as the penalties are larger. Thus, it could be possible to see crimes such as malware and fraud appear to increase relative to all spam sent, as the less serious spammers desist from sending spam.

Cyberspace may have different implications for deterrence theory than can be expected from deterrence in physical space.[21] Digital space is governed by different physics, as computer networks are unbounded, infinitely scalable, and abstract. In physical space, both modalities for attack and the severity of outcomes scale consistently and predictably. However, in cyberspace, an offender can scale infinitely, as a small-time offender can acquire as large a botnet as their skillset and determination allow.

There has been some empirical testing of deterrence theory as applied to cybercrime. Prosecution and law enforcement activity against cybercriminals has been linked to reductions in hacking incidences, cyberattacks on businesses, and Distributed Denial of Service (DDoS) attacks.[22] Prosecutions of spammers specifically have been linked to reductions in spam sent and increased compliance with certain spam laws among spammers.[23] However, it is uncertain the impact that prosecutions of spammers might have on more serious offenses carried out via spam technology, such as malware and fraud.

Methodology.

A dataset built from a sample of spam emails was created to investigate the impact the CAN SPAM Act has had on malware and fraud facilitated by spam. One measure of fraud and two measures of malware distribution were used. Emails were classified as fraudulent by a spam filter repurposed to identify fraud. Malware was either measured as the inclusion of malicious links in an email body or as executable scripts embedded in the email.

Sample and Data.

The sample, that of spam emails, was taken from publicly available spam archives from which spam emails are collected and stored for subsequent download by researchers. The data were retrieved from the Untroubled Software website on December 18, 2013.[24] The available spam archives were collected by posting multiple "honey net" email addresses publicly online for spam crawlers to harvest. The honey net approach was intended to bait spammers to add a given email address to a spam listserv, with the goal of intentionally receiving spam emails. When an email address is posted on Internet websites such as forums, message boards, and on personally hosted web pages, web bots may scan and identify them as email addresses, extract them, and store them in a spamlist or database for subsequent spam targeting.

The data collected includes a purposive sample of all individual spam emails hosted for download that were received in bait honeypot email accounts between March 1998 and November 2013, totaling 5,490,905 email messages. Each email is encoded in an individual text file containing the contents of the spam email, which includes header information, the body of the message including any scripts or Hypertext Markup Language (HTML), and any file attachments the email contained, converted to a plain text format stored at the end of the file with an encoding scheme termed "BASE64."

Procedures.

In order to be analyzed in a time series design, the spam email sample was coded by the date it was received. Software was written in Java to parse each message in the sample to code the messages on this dimension. The data points were then extracted by the software and saved in a tabular dataset for cleaning and analysis. Each row of the dataset represents an individual spam email message, with 5,490,905 rows total.

The contents of the spam data was imported into SPSS (statistical analysis) software in order to be aggregated into a monthly time series dataset and aggregated by month, subsequently shrinking the size of the dataset to 189 observations, as there were 189 months in the sample. The smaller dataset was then exported to R (statical analysis software) for analysis.

Measures and Variables.

There are three sets of measures that are included in subsequent models. The first set includes the dependent variables, that being the measures of fraud and malware. The second set includes independent variables representing CAN SPAM Act activity, including enforcement, CAN SPAM Act attention and public awareness, attitudes toward the CAN SPAM Act, and lack of spammer anonymity due to attribution to the spammer's identity in the news. Finally, a number of economic and technological time series predictors are available for inclusion in each model, to serve as control variables. Each of these is thought to possibly relate to spam or illegal behavior in some way and is discussed in more detail in the following sections.

Dependent Variables: Fraud and Malware.

The dependent variables, fraud and malware, were extracted by the spam mining software discussed in the procedures outlined in the previous section. A single measure of fraud and two measures of malware distribution were coded for by the software. All measures were lagged by 1 month in all subsequent regression analyses.

Fraudulent Spam Message. The software uses a repurposed spam filter to calculate the probability that a message is fraudulent rather than non-fraudulent. Spam filters are used to calculate the probability that a message received is spam, as opposed to legitimate email that users want to receive/read (termed "ham" emails). Spam filters typically are trained on a sample of two data sources, a collection of spam emails that are already known to be spam, as well as a collection of ham emails (legitimate messages) a coder has already identified as legitimate. Spam filters scan the two data sources and calculate base probabilities that a given keyword found in an email is spam based on the keyword frequencies found in these two training data samples. The spam filter can then predict the probability that a new set of emails are spam, based on these probabilities.

The spam filter employed for this chapter is a naïve Bayes classifier, which attempts to classify an instance of text as either being in one of two dichotomous categories based on trained probabilities associated with the text's keyword frequencies.[25] To calculate the probability that the keyword is associated with a category, the probabilities that a keyword is found in fraudulent emails must first be analyzed. An existing open source naïve Bayes spam filter was acquired from the Code Project website.[26] The software was written in C# and was repurposed to create a dataset of trained probabilities that a word is found in a fraudulent message.

There was a two-step process in order to employ fraud classification on the spam archives data sample: training the base keyword probabilities, and then incorporating those probabilities into the software that can calculate whether an email instance is fraudulent. The training of the classifier was performed using two spam email samples, one taken from the spam archives itself, and the other pulled from a separate fraud spam database available online. One thousand spam emails were taken from the existing spam archives used in this sample that were confirmed via a human rater to be non-fraudulent in nature. The sample was used as the non-fraudulent training sample and was excluded from the final dataset building process by the software to avoid classifying messages the software was trained on.

The second sample, consisting of fraudulent training emails, was pulled from the Scamdex website, which hosts a publicly available database of user-submitted reports of email scam contents.[27] Because the accuracy of a spam filter can degrade if the sample used to train the classifier is older than the new messages it is intended to scan, fraudulent spam messages were sampled from the years 1998 to 2013 in order to capture a temporally wide range of messages.[28] A total of 2,339 scam messages were downloaded to be used as a scam training sample.

The fraud probability measure was aggregated into a time series variable representing the percent of emails with 85 percent or higher predicted probabilities of being fraudulent per month. The measure was not found to be trend stationary (*Dickey-Fuller* = -1.41, p = .82). Regular differencing resulted in significant stationarity (*Dickey-Fuller* = -8.26, $p < .01$) per month. For details on this methodology, see the Analytic Plan section of this chapter.

Executable Download Link. Likely, a more common attack vector involving the distribution of malware in spam is the inclusion of malicious web links. Because the email client is not able to scan or detect the scripts or executable nature of the website the user is being linked to, the local software or mail server is less able to warn and protect the recipient from following a link that looks suspicious. A common method is the drive-by-download, where simply visiting a web page with the recipient's browser launches scripts on that page that exploit a vulnerability in the user's browser that automatically downloads and installs malicious software hosted on the web server.

While this is a popular and effective method among cybercriminals for malware distribution, it is beyond the scope of the spam mining software, since the spam sample dates back to 1998, in which case most of the malicious links or websites are certainly no longer online today and cannot be verified to be malicious. Instead, the software detected if an email was linked directly to a file download and would determine if the file extension was executable if it matched a list of known executable file extensions. The list of executable file extensions used was found on the About.com website.[29]

Linking directly to a malicious file download usually does not exploit any vulnerability that triggers an automatic install after download. Instead, the file is downloaded, and it is up to the spam recipient whether they choose to open the file or not. A limitation is that a link may not directly include the filename in the URL, but instead, may dynamically route the victim to a downloadable file after following the link. However, for the purposes of this research, the software only detected direct download links, although that may bias the data in favor of more novice malware distributors.

The software matched any text that begins with "http://" and ends with a dot (".") followed by an executable file extension that matched the available list of executable file extensions. The first executable link found in the email was recorded and coded "1" for executable download link found, otherwise it was coded "0."

HTML Scripts. A second means in which emails can be used to distribute malware is by running executable scripts that are embedded in the email itself that the email client, not the operating system or web browser per se, executes. Emails can be formatted with HTML, the same language used to design web pages. HTML can also include script tags, which an

HTML interpreter or script engine, such as that in a web browser or email client, can execute. Most email clients disable running scripts in email because of its possibility for abuse, so it is rare for an email sender to include script tags in an email. When an email does include such tags, it is likely for malicious purposes, such as installing malware.

The software matched any opening script tags embedded in the email body, or if applicable, any attached HTML files in the email. If the software matched "<script" followed by zero or more of any character of any length so long as there is no line break, ending with a closing bracket (">"), the software coded an executable script tag variable as "1" for true; otherwise, it was coded "0."[30] The measure was then aggregated by month as the percent of emails with executable script tags over time.

Independent Variables: CAN SPAM Act Activity.

The impact to test is the activity, enforcement, and attention of and toward the CAN SPAM Act. Most of the measures are taken from news and media attention about the CAN SPAM Act, but an additional time series metric has been created from Google search history data. Theoretical underpinnings of deterrence regarding the CAN SPAM Act were intended to be captured and tested with the independent measures, including: attention toward CAN SPAM convictions and monetary damages won; attribution and lack of anonymity of spammers in the media; news that is critical of the CAN SPAM Act versus news that is not; as well as Internet search activity of the CAN SPAM Act.

All measures that derived from news reports on the CAN SPAM Act were acquired from a series of

LexisNexis searches. The search results were limited to only those news sources that are located within the United States. All 347 unique news articles that were returned from a combination of CAN SPAM search terms (can spam act, can-spam, etc.) were downloaded and coded on the four sets of measures that derived from news sources. The coded measures were tested for inter-rater agreement.

CAN SPAM Act Enforcement. The quantity and severity of CAN SPAM Act enforcement highlighted by the media were captured from news results, such as the number of prosecutions, convictions, the amount of damages awarded during lawsuits. There were nine time series measures of CAN SPAM Act enforcement and deterrence from news articles. They included two measures of damages awarded (the total U.S. dollars [USD] awarded per month and the count of articles awarding damages per month). There were also two measures of spammer detentions, including the sum of days spammers were detained per month, and the count of articles mentioning spammer detentions. The number of spammer arrests per month was also recorded. There were also three count variables representing trials under the CAN SPAM Act: the number of convictions, acquittals, and then-ongoing and unresolved trials. Finally, the percentage of articles relating to the CAN SPAM Act per month was recorded; not all of the articles were related to the CAN SPAM Act, but they were related to spam.

News Critical of the CAN SPAM Act. Much of the initial attention the CAN SPAM Act received when it was introduced was not positive about the Act's effectiveness.[31] Naturally, this kind of reporting could have the opposite effect of deterrence, emboldening spammers located in the United States. Three time series measures were constructed to capture attitudes toward the CAN SPAM Act: the percent of articles that were positive, negative, or neutral about the CAN SPAM Act. The same was done for author attitudes about spam in general. That is, whether authors' attitudes were positive, negative, or neutral about society's ability to fight spam.

Attribution of Spammers. The impersonal and anonymous nature of crimes perpetrated in cyberspace, such as that of spam, can attenuate some of the deterrent effect a legal punishment might impose. Attribution of cybercriminal identities in the news can reduce some of the feelings of anonymity online. That is, news that mentions the identity of a specific cybercriminal, rather than discussing cybercrime in general. Attribution of cybercriminals at the national level has been associated with fewer cybercrime attacks within those countries.

Dichotomous Impact of the CAN SPAM Act. A simpler measure of the CAN SPAM Act was also used, representing a before and after intervention variable representing the months in which the CAN SPAM Act was being enforced and in effect as a law. The measure is coded "0" for any time before the Act went into enforcement on January 1, 2004, and "1" following this date.

Google CAN SPAM Act Search History. Google offers reporting of time series plots for popular terms searched for using the Google search engine, called Google Trends.[32] It is suspected that Google searches for the CAN SPAM Act ought to reflect public awareness of the law. Multiple time series of different CAN SPAM search queries (e.g., "can spam," "can spam act," "can-spam act") were downloaded from the Google Trends service and merged into a single time series representing the count of all searches related to the CAN SPAM Act per month. Searches were limited to only those within the United States.

Control Variables: Technological, Economic, and Demographic Predictors.

Possible influences on spam from sources other than enforcement and awareness of the law were also taken into account. There were three groupings of control variables included: technological, economic, and demographic/other time series predictors. Controlling for such measures enhanced any certainty that the CAN SPAM Act did or did not have an impact on spam volume. Any observations with missing data points have been interpolated.

Technological predictors included the:

- Number of Internet users per capita;[33]
- Number of technology jobs in computer systems and related services;[34] and,
- Wilshire Internet Market Index. [35]

The Wilshire Index measures the price and the total returns on investments (the performance) of publicly traded Internet stocks. All three measures were found to not be sufficiently trend stationary (respectively: *Dickey-Fuller* = -2.13, p = .52; *Dickey-Fuller* = -2.66, p = .3; and *Dickey-Fuller* = -2.3, p = .45). Regular differencing resulted in stationarity (*Dickey-Fuller* = -5.66, p < .01; *Dickey-Fuller* = -6.76, p < .01; and *Dickey-Fuller* = -5, p < .01).

Six economic predictors were included, composed of:

- Real disposable personal income per capita;[36]
- Gross Domestic Product (GDP) growth rates;[37]
- U.S. unemployment rate;[38]
- Percent of the population with a college degree;[39]
- Consumer Price Index (CPI);[40] and,
- Financial Stress Index (FSI).[41]

The CPI measures the inflation level and spending power of the average U.S. household to purchase from a fixed list of consumer goods. The FSI measures the amount of financial stress in the markets and is built from 18 time series datasets capturing interest rates, yield spreads, and other indicators. Five of the variables—income, GDP, unemployment, CPI, and FSI—were found to be serially correlated (respectively: *Dickey-Fuller* = -.71, p = .97; *Dickey-Fuller* = -2.99, p = .16; *Dickey-Fuller* = -2.13, p = .52; *Dickey-Fuller* = -2.49, p = .37; *Dickey-Fuller* = -2.96, p = .17). Regular differencing resulted in significant stationarity (*Dickey-Fuller* = -5.78, $p < .01$; *Dickey-Fuller* = -4.23, $p < .01$; *Dickey-Fuller* = -8.21, $p < .01$; *Dickey-Fuller* = -6.4, $p < .01$; *Dickey-Fuller* = -5.81, $p < .01$).

Three additional demographic and other variables consisted of:

- Total population size per month;[42]
- Younger population aged 15-24;[43] and,
- Uniform Crime Report (UCR) arrest rates per 100,000 individuals in the population.[44]

These variables tend to relate to street crime, so it is considered whether they also relate to the cybercrime offense of sending spam. Both the general population

(*Dickey-Fuller* = -2.08, *p* = .54) and younger population (*Dickey-Fuller* = -.76, *p* = .97) measures were found to be serially dependent. Differencing results in significant stationarity for both (*Dickey-Fuller* = -20.85, *p* < .01; *Dickey-Fuller* = -6.54, *p* < .01).

Analytic Plan.

Multiple generalized least squares (GLS) regression models were conducted to test the impact the CAN SPAM measures have on fraud and malware lagged by 1 month. GLS allows for a non-constant variance among the residuals to be controlled for, as may be the case in time series models due to serial correlation of the residuals.[45] Predictor variables included in each of the three regression models were selected via backward stepwise regression based on the model Akaike information criterion (AIC). Stepwise regression ends once elimination of a predictor results in a higher AIC score. Predictors that increase the AIC score when eliminated were retained; all three regression models were used and started with 33 independent and control variables.

With each of these models specified, the residuals were tested to investigate signs of serial autocorrelation. Autocorrelation and partial autocorrelation were tested in the residuals for each model; and for any substantial serial correlation, autoregressive or moving average arguments were specified in final GLS models to account for heteroscedasticity.[46] This process was repeated for each regression model, one for each of the three spam outcome series.

Results.

Inter-rater Reliability Testing: CAN SPAM IV.

The coded CAN SPAM Act news articles were also tested for inter-rater agreement. Of the 347 LexisNexis articles, 100 were randomly selected and coded a second time by an additional rater. There was sufficient agreement on whether the article related to the CAN SPAM Act or just spam in general (*Kappa* = .88, p < .001) and whether author attitudes toward the act were positive, neutral, or negative (*Kappa* = .82, p < .001). The agreement of author attitudes toward spam in general (positive, neutral, or negative) was significant (*Kappa* = .68, p < .001), but slightly lower than the .7 cutoff. There was high agreement on trial status (ongoing trial, conviction, acquittal) (*Kappa* = .83, p < .001) and whether the spammer was detained (*Kappa* = .93, p < .001). There was perfect agreement on whether the spammer was arrested (*Kappa* = 1, p < .001) and on whether damages were awarded (*Kappa* = 1, p < .001). Finally, there was substantial agreement on whether the identity of a given spammer was known (attribution) (*Kappa* = .87, p < .001). The coded measures were considered reliable and thus included in subsequent analyses.

Fraudulent Spam Prediction Performance.

The accuracy of the measure of fraud used required testing to determine its predictive power. A random sample of 200 spam emails from the entire spam sample was selected for testing the classifier. The 200 emails were manually read and coded as either fraudulent or non-fraudulent by a human rater. The Receiver Operating Characteristic (ROC) Area Under the Curve (AUC) was selected as the performance metric to be used to compare the agreement between the human coder and the naïve Bayes classifier.[47] The AUC typically ranges from .5 to 1.0, with a score of .5 being no better than a coin toss at correctly classifying a case and 1.0 being perfect predictive accuracy. The AUC yielded a score of .83, suggesting strong predictive performance of the measure of fraud.

Multivariate Analyses: Time Series Regression of Percent Fraudulent Emails Per Month. A backward stepwise regression using the model AIC was conducted with the percentage of emails classified as fraudulent per month regressed on an initial 33 predictor variables total. Backward elimination yielded 9 predictor variables to be included in the final time series model. The selected predictors were included in a linear regression and the residuals were computed to test for autocorrelation. A Durbin Watson test of the residuals found no evidence of significant autocorrelation (dw = 2.65, p = 1).

After inspection of the autocorrelation (ACF) and partial autocorrelation (PACF) correlograms of the regression, an autoregressive moving average (ARMA) model was identified—ARMA(1,1). A correlogram is a visual plot of the correlation between a time series and itself at a given lag, for successive increments of lags one and up.[48] The ACF is a simple correlation of a time series with itself at a given lag, while a PACF represents the correlation of a time series with itself at lag k, controlling for all lags in between itself and lag k. While differencing of the data is sufficient to create a trend stationary time series process, there may still be some degree of serial dependency in the data. ACF and PACF functions can reveal such serial dependency and indicate that said processes need to be controlled for in any subsequent regression models. If there are *q* spikes in an ACF correlogram, a moving average model of order *q* should be controlled for (ARMA[0,*q*]). If there is a decay pattern in the ACF function, an autoregressive parameter at order *p* should be controlled for (ARMA[*p*,0]), *p* being inversely proportionate to the speed of decay. The reverse interpretation is required of the PACF correlogram, with a spike indicating an autoregressive process and decay patterns indicating a moving average process. A final GLS time series regression model was run using the nine selected predictors, shown in Table 3-1.

Measure	***Beta***	***SE***	***t***	***p-value***
Intercept	.042	.026	1.58	.1159
UCR Arrest Rate	.107	.025	4.213	< .0001***
Percent Internet Users	-.137	.047	-2.908	.0041**
Unemployment Rate	-.116	.034	-3.433	.0007***
Technology Jobs	-.072	.011	-6.446	< .0001***
Population Aged 15-25	-.171	.074	-2.304	.0224*
CPI	-.06	.026	-2.277	.024*
Count of Trial Spammer Acquitted Articles	.059	.05	1.172	.2428
Percent of Articles Negative About CAN SPAM	-.007	.013	-.532	.5955
Percent of Articles without Spammer Attribution	.006	.018	.339	.735

R^2 = 5.81%

* < .05, ** < .01, *** < .001

Table 3-1. Generalized Least Squares (GLS) Time Series Regression of Percent Fraudulent Per Month, ARMA(1,1) n = 189.

Arrest rates predict a higher amount of fraud (*B* = .107, *p* < .0001). Street crime and fraud cybercrime appear to be correlated. More Internet users predicts a reduction in fraud (*B* = -.137, *p* = .004). It should be noted that higher proportions in Internet users are also associated with less spam being sent and increased spam regulation compliance. The pattern seems to suggest that more Internet users reduce the severity of cybercrime within the United States. Technology jobs also predict a reduction in fraud (*B* = -.072, *p* < .0001).

However, while more technology jobs decreases fraud, lower unemployment increases it (*B* = -.116, *p* = .0007). CPI is also significant and predicts less fraud (*B* = -.06, *p* = .024). There is little consistency with the economic predictors of unemployment, technology jobs, and CPI, other than they all predict a reduction in fraud. However, unemployment represents a struggling economy, while the remaining two predictors indicate stronger economies. Finally, youth population size is associated with less fraud (*B* = -.171, *p* = .022). The direction of this relationship is not consistent with a priori predictions that higher youth populations predict increases in crime.

Time Series Regression of Percent of Spam with Malicious Links Per Month. A backward stepwise regression using the model AIC was conducted with the percentage of emails containing links to executable files per month regressed on an initial 33 predictor variables total. Backward elimination yielded five predictor variables to be included in the final time series model. The selected predictors were included in a linear regression and the residuals were computed to test for autocorrelation. A Durbin Watson test of the residuals found significant autocorrelation (*dw* = 1.13,

p < .001). Regular differencing of the variables in the model resulted in sufficient trend stationarity (dw = 2.86, p = 1). After inspection of the ACF and PACF correlograms of the regression, an ARMA(0,2) model was identified. A final GLS time series regression model was run using the five selected predictors, shown in Table 3-2.

Measure	*Beta*	*SE*	*t*	*p-value*
Intercept	.001	.015	.064	.9487
Unemployment Rate	.072	.091	.79	.4304
Count of Spammers Arrested	-.128	.067	-1.913	.0574†
Count of Trial Ongoing Articles	.165	.086	1.92	.0564†
Count of Damages Awarded Articles	-.205	.09	-2.278	.0239*
Percent of Articles with Spammer Attribution	.13	.044	2.981	.0033**

R^2 = 8.16%
* < .05, ** < .01, *** < .001, † < .1

Table 3-2. Generalized Least Squares Time (GLS) Series Regression of Percent of Spam with Malicious Links Per Month, ARMA(0,2) n = 189.

The count of articles mentioning damages being awarded and judged against a spammer per month is associated with a decrease in malicious links (B = -.205, p = .024). The relationship is in the theoretically expected direction and it would suggest a deterrent effect. However, the percentage of articles with spammer attribution predicts an increase in malicious links (B = .13, p = .003). The relationship is opposite the theoretically expected direction.

It should be mentioned that two other predictors in the model were not quite significant. The count of articles mentioning arrests of spammers per month predicts a reduction in malicious links (*B* = -.128, *p* = .057). The count of ongoing trials mentioned in the news per month predicts an increase in malicious links in the spam sample (*B* = .165, *p* = .056). The two measures that predict a decrease in malicious links both represent punishments of spammers (arrests and fines). The two measures that predict an increase in malicious links do not necessarily pertain to punishments of spammers (ongoing trials and attribution). The attribution articles mention spammer identity, but do not necessarily involve punishments, and may even describe spammers being acquitted. The attribution measure may be similar to the ongoing trial measure in this way, and so they may not have a deterrent effect. Punishment in the news, however, may be a deterrent to this type of cybercrime.

Time Series Regression of Percent of Spam with Embedded Scripts Per Month. A backward stepwise regression using the model AIC was conducted with the percentage of emails containing embedded script tags per month regressed on an initial 33 predictor variables total. Backward elimination yielded five predictor variables to be included in the final time series model. The selected predictors were included in a linear regression and the residuals were computed to test for autocorrelation. A Durbin Watson test of the residuals found significant autocorrelation (*dw* = .89, *p* < .001). Regular differencing of the variables in the model resulted in sufficient trend stationarity (*dw* = 2.36, *p* = .99). After inspection of the ACF and PACF correlograms of the regression, an ARMA(0,2) model was identified. A final GLS time series regression model was run using the five selected predictors, shown in Table 3-3.

Measure	*Beta*	*SE*	*t*	*p-value*
Intercept	< .0001	.032	-.004	.997
Percent Internet Users	-.088	.045	-1.966	.0508†
Percent Population Aged 15-25	-.236	.071	-3.335	.001**
Count of CAN SPAM Articles	-.144	.057	-2.506	.0131*
Count of Spammer Detained Articles	.067	.044	1.509	.133
Percent of Articles without Spammer Attribution	.071	.031	2.294	.0229*

R^2 = 17.15%
* < .05, ** < .01, † < .1

Table 3-3. Generalized Least Squares (GLS) Time Series Regression of Percent of Spam with Embedded Scripts Per Month, ARMA(0,2) n = 189.

The percent of the population aged 15-25 is associated with a decrease in embedded script tags per month (*B* = -.236, *p* = .001). The number of articles on the CAN SPAM Act published per month predicts a decrease in embedded scripts (*B* = -.144, *p* = .013), consistent with what might be expected from a deterrent effect. The percentage of articles without spammer attribution predicts an increase in malicious scripts (*B* = .071, *p* = .023), consistent with the emboldening effect of feelings of anonymity. However, attribution was found to increase malicious links in the prior model. Attribution appears to have the opposite effect on malicious scripts, although the effect size is very small.

Finally, the percent of the population who are Internet users does not quite achieve significance, but is associated with a decrease in embedded scripts (*B* = -.088, *p* = .051). The direction of the relationship is consistent with all significant findings involving this variable in prior models. Internet connectivity appears to reduce the negative effects of illicit spam.

DISCUSSION

Three time series models capturing fraud and malware activity among email spammers received within the United States were constructed to test the impact that prosecuting spammers might have on such crimes. While prosecuting spammers has been associated with reductions in spamming offenses in prior literature, it was questioned whether the same law enforcement activity against spammers might also have an impact on more serious forms of cybercrime perpetrated through email spam. The results suggest a possible impact of the CAN SPAM Act on malware contained in email spam, although there appears to be little evidence of an impact on fraudulent spam.

IMPLICATIONS OF FINDINGS

The CAN SPAM Act and other deterrent influences appear to have little impact on email fraud, yet are predictive of malware distribution among the spam email sample. Regarding the fraudulent email model, there were no CAN SPAM Act or deterrent related predictors that predicted the fraud outcome chosen. It may be that email spammers who reside in the United States are not as likely to rely on fraud, but rather rely more heavily on "spamvertised" goods and products. Fraudulent emails received in the United States may be more likely to originate from other countries (Nigeria, Russia, etc.), and therefore, the fraudsters would likely not even read U.S. news on the CAN SPAM Act, let alone be influenced by it.

Fraud, being a more serious offense than electronic spam violations, is also a more risky crime to commit.

Given that the offense is already more serious and associated with higher risk, offenders may be less prone to deterrent influences. More serious offenders may be less likely to be deterred, as they have already taken on greater risk than less serious offenders by the nature of their crimes. Assuming the measure of fraud is valid, the CAN SPAM Act seems to have little effect.

For the malware distribution models, however, deterrence efforts may have an impact. Yet the direction of effect size is not consistent with the malicious links model. Arrests and fines under CAN SPAM Act prosecutions reduce the number of malicious links, while ongoing trials and attribution increases malware. It may be that articles mentioning punishments of spammers deter malicious links, whereas articles only mentioning spammer identities (attribution) and ongoing trials without a punishment increase malicious links. Yet, attribution decreases malware in the malicious scripts model, even though it increases malware in the malicious links model. These two types of attack vectors for distributing malware may be different from each other such that deterrent efforts may have different impacts on them.

The two influences of malicious scripts were consistent with deterrence, though, with CAN SPAM articles and attribution predicting reduced malicious scripts. Neither of these measures necessarily mentions punishments of spammers. Regardless of effect size direction, the CAN SPAM Act appears to influence malware, whereas it has no effect on fraud. There also appears to be no evidence of a marginal deterrent effect, with an increase in severity associated with a deterrent stimulus. That is, a threat of punishment might deter minor offenders, but not more serious offenders; ultimately resulting in more remaining serious offenders. Prior research has suggested such a marginal deterrent influence when the measure of cybercrime is a DDoS attack, yet the same does not appear to be the case when looking at fraud and certain types of malware distribution.[49]

LIMITATIONS

The spam sample and the procedures for extracting the time series metrics from the sample have some limitations that ought to be mentioned. The sample itself was acquired from only a single web archive, collected by an uploader, which may not have been completely consistent in the process for baiting spam messages during the entire 16 years of data collection.[50] That is, changes might have been made or slowly introduced, such as the number or frequency of bait email addresses or address posts on the Internet made over time. While the data ought to reflect genuine spamming activity, there may be fluctuations or systematic changes in time for different observations that would not be accounted for by the existing predictors in the model.

The spam sample used might also be skewed toward certain spammers who send more spam than usual to the same recipient's inbox. For the individual email unit of analysis dataset, each observation is not independent of other observations or spam that was received. That is, multiple emails can easily be sent by the same spammer, and many of those emails are likely identical to each other in the types of variables coded by the spam software. So the sample is biased toward spammers who send more spam to the same recipient. This is likely another example where the data is more representative of more serious, unlawful spammers.

The measures of malware can also be improved. The methods used to detect malware were simply rule-based classification methods, identifying a message as malicious based on a single defining feature per each outcome. Machine learning techniques similar to those employed to detect fraud ought to be considered when classifying a message as being malicious, since those methods can rely on much more information than a simple single-rule based scheme. Specifically, a classification algorithm ought to account for many features that are evidence of malware, as there are many hundreds of different defining characteristics that separate malicious emails from non-malicious ones.

CONCLUSION

This chapter has investigated the possible deterrent impact the CAN SPAM Act might have had on the more serious forms of cybercrimes, which were carried out through electronic spam. The evidence suggests no influence of the Act on the measure of fraud chosen, but some potential influence on malware distributed through email spam. Future research, some of which is presently underway, ought to expand on the measures of fraud and malware chosen. Specifically, fraud can be split into several separate categories, such as phishing and advance fee fraud. Malware can also be identified through more sophisticated machine learning methods. Links contained in spam emails can also be identified as malicious by cross-referencing them with existing databases of blacklisted malicious URLs.

In addition, research ought to investigate the impact of prosecuting perpetrators of fraud and distributors of malware on more serious forms of cybercrime.

While the current study yielded mixed findings in terms of the impact of prosecuting spammers on fraud and malware in spam, legal punishments of serious cybercriminals could lead to different results. The present findings shed some light on the nature of fraud and malware contained in spam, and warrants further exploration.

ENDNOTES - CHAPTER 3

1. An earlier version of this chapter appeared as the paper Alex Kigerl, "Malicious Spam: The Impact of Prosecuting Spammers on Fraud and Malware Contained in Email Spam," Presented at The City University of New York (CUNY), City College, Cyber Infrastructure Protection (CIP) Conference in New York on October 15, 2015.

2. Darya Gudkova, "Kaspersky security bulletin: Spam evolution 2012," Securelist, January 21, 2013, available from *www.securelist.com/en/analysis/204792276/Kaspersky_Security_Bulletin_Spam_Evolution_2012*, accessed April 29, 2013.

3. Ivan P. L. Png and Chen-yu Wang, "The Deterrent Effect of Enforcement Against Computer Hackers: Cross-Country Evidence," Paper presented at the Sixth Workshop on the Economics of Information Security, Pittsburgh, PA, June 7-8, 2007.

4. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), 15 U.S.C. §§ 7701-7713, 2005.

5. Alex C. Kigerl, "Evaluation of the CAN SPAM Act: Testing Deterrence and Other Influences of E-mail Spammer Legal Compliance Over Time," *Social Science Computer Review*, Vol. 33, Iss. 4, October 2014, available from *http://journals.sagepub.com/doi/full/10.1177/0894439314553913*.

6. Vikas Lachhwani and Sanjoy Ghose, "Online information seeking for prescription drugs," *International Journal of Business and Systems Research*, Vol. 6, No. 1, 2012, pp. 1-17.

7. Justin M. Rao and David H. Reiley, "The Economics of Spam," *The Journal of Economic Perspectives*, Vol. 26, No. 3, Summer 2012, pp. 87-110.

8. Symantec Corporation, "Internet Security Threat Report: 2014," *2013 Trends*, Vol. 19, Mountain View, CA: Symantec Corporation, April 2014.

9. Kindsight Security Labs, "Kindsight Security Labs Malware Report Q2 2012," Mountain View, CA: Kindsight Incorporated, 2012.

10. Trendlabs, "Turning the Tables on Cyber Attacks: Responding to Evolving Tactics," *TrendLabs 2Q 2014 Security Roundup*, Trend Micro Incorporated, 2014.

11. Kaspersky, "Security in a multi-device world: the customer's point of view," Kaspersky Lab, 2013.

12. Solutionary, "Global Threat Intelligence Report," Omaha, NE: Solutionary, March 12, 2013.

13. Internet Crime Complaint Center (IC3), *2013 Internet Crime Report,* Washington, DC: Internet Crime Complaint Center, Federal Bureau of Investigation, 2014, available from *https://www.ic3.gov/media/annualreport/2013_IC3Report.pdf*.

14. EMC and RSA, "2013 A Year in Review," *Fraud Report*, Report No. JAN RPT 0117, EMC Corporation, 2014.

15. Cyveillance, "The Cost of Phishing: Understanding the True Cost Dynamics Behind Phishing Attacks," *A Cyveillance Report*, Arlington, VA: Cyveillance Incorporated, October 2008.

16. Ponemon, "2013 Cost of Cyber Crime Study: United States," *Ponemon Institute Research Report*, Traverse City, MI: Ponemon Institute Limited Liability Corporation, October 2013.

17. Ultrascan, "419 advance fee fraud statistics 2013," Ultrascan Advanced Global Investigations, 2014.

18. Noel Otu, “Kidnapping: A Variant of Nigerian Advance Fee Fraudsters (419) Diversified Portfolio,” *International Journal of Criminal Justice Sciences*, Vol. 8, Iss. 1, January-June 2013.

19. Jack P. Gibbs, *Crime, Punishment, and Deterrence*, New York: Elsevier Science Limited, 1975.

20. Franklin E. Zimring and Gordon J. Hawkins, *Deterrence: The legal threat in crime control,* Chicago: University of Chicago Press, 1973.

21. Kim A. Taipale, “Cyber-deterrence,” *Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital And Internet Immobilization*, IGI Global, 2010.

22. Clement Guitton, “Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence,” *International Journal of Cyber Criminology*, Vol. 6, No. 2, July-December 2012.

23. Alex C. Kigerl, “Deterring Spammers: Impact Assessment of the CAN SPAM Act on Email Spam Rates,” *Criminal Justice Policy Review*, Vol. 27, Iss. 8, 2016, first pub. December 22, 2014, available from *http://dx.doi.org/10.1177/0887403414562604*.

24. Untroubled Software website, available from *https://untroubled.org/.*

25. Drew Conway and John Myles White, *Machine Learning for Hackers: Case Studies and Algorithms to Get You Started*, Sebastopol, CA: O’Reilly Media, Incorporated, 2012.

26. Code Project website, available from *http://www.codeproject.com/KB/recipes/BayesianCS.aspx*, accessed September 12, 2010.

27. Scamdex website, available from *http://www.scamdex.com*.

28. Gordon V. Cormack and Jose-Marcio Martins da Cruz, “On the relative age of spam and ham training samples for email filtering,” in *SIGIR ‘09: Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval,* Boston, MA: Association for Computing Machinery, 2009, pp. 744-745.

29. Tim Fisher, "List of Executable File Extensions: An Incomplete List of Executable File Extensions," Lifewire, About.com, available from *https://www.lifewire.com/list-of-executable-file-extensions-2626061*, accessed March 21, 2013.

30. Scripts in emails tend to be of the form "<script language='JavaScript'>" and so the pattern matcher would identify such text.

31. Vivek Arora, "The CAN-SPAM Act: An Inadequate Attempt to Deal with a Growing Problem," *Columbia Journal of Law and Social Problems*, Vol. 39, No. 3, Spring 2006, pp. 300-330; Galen A. Grimes, "Compliance with the CAN-SPAM Act of 2003: Studying the application of the CAN-SPAM Act and its effect on controlling unsolicited email messages," *Communications of the ACM*, Vol. 50, Iss. 2, 2007, pp. 56-62; Younghwa Lee, "The CAN-SPAM Act: A silver bullet solution?" *Communications of the ACM*, Vol. 48, No. 6, 2005, pp. 131-132; Tom Zeller, Jr., "Law Barring Junk E-mail Allows a Flood Instead," *The New York Times*, February 1, 2005, p. A1.

32. Google Trends, "Visualizing Google data," available from *http://www.google.com/trends*.

33. Pew Internet Research Center website, available from *http://www.pewinternet.org/*.

34. U.S. Bureau of Labor Statistics, "All Employees: Professional and Business Services: Computer Systems Design and Related Services (CES6054150001)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/CES6054150001*, accessed December 17, 2013.

35. Wilshire Associates, "Wilshire Internet Total Market Index© (WILLWWW)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/WILLWWW*, accessed December 17, 2013.

36. U.S. Bureau of Economic Analysis, "Real Disposable Personal Income: Per Capita (A229RX0Q048SBEA)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/A229RX0Q048SBEA*, accessed December 18, 2013.

37. Organization for Economic Co-operation and Development, "Quarterly National Accounts: Quarterly Growth Rates of real GDP, change over previous quarter," OECD.Stat, available from *https://stats.oecd.org/index.aspx?queryid=350*, accessed December 26, 2013.

38. U.S. Bureau of Labor Statistics, "Civilian Unemployment Rate (UNRATE)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/UNRATE*, accessed December 17, 2013.

39. U.S. Bureau of Labor Statistics, "Civilian Labor Force Participation Rate: Bachelor's Degree and Higher, 25 years and over (LNU01327662)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/LNU01327662*, accessed December 25, 2013.

40. U.S. Bureau of Labor Statistics, "Consumer Price Index for All Urban Consumers: All Items (CPIAUCSL)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/CPIAUCSL*, accessed December 18, 2013.

41. Federal Reserve Bank of St. Louis, "St. Louis Fed Financial Stress Index© (STLFSI)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/STLFSI*, accessed December 18, 2013.

42. U.S. Bureau of the Census, "Total Population: All Ages including Armed Forces Overseas (POP)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/POP*, accessed December 17, 2013.

43. Organization for Economic Co-operation and Development, "Working Age Population: Aged 15-24: All Persons for the United States© (LFWA24TTUSM647S)," FRED, Federal Reserve Bank of St. Louis, available from *https://fred.stlouisfed.org/series/LFWA24TTUSM647S*, accessed December 17, 2013.

44. NACJD, "Uniform Crime Reporting Program Resource Guide," available from *www.icpsr.umich.edu/icpsrweb/content/NACJD/guides/ucr.html*, accessed December 25, 2013.

45. George G. Judge, William E. Griffiths, Rufus Carter Hill, Helmut Lütkepohl, and Tsoung-Chao Lee, *The Theory and Practice of Econometrics*, 2nd Ed., New York: Wiley, 1986.

46. A. Ian McLeod, Hao Yu, and Esam Mahdi, "Time Series Analysis with R," *Handbook of Statistics*, Vol. 30, 2012.

47. Tom Fawcett, "ROC Graphs: Notes and Practical Considerations for Researchers," *Machine learning*, Vol. 31, 2004, pp. 1-38.

48. David McDowall, Richard McCleary, Errol E. Meidinger, and Richard A. Hay, Jr., *Interrupted Time Series Analysis*, Sage University Paper series on Quantitative Applications in the Social Sciences, No. 21, Thousand Oaks, CA, and London: Sage Publications, 1980.

49. Kai-Lung Hui, Seung Hyun Kim, and Qiu-Hong Wang, "Marginal Deterrence in the Enforcement of Law: Evidence from Distributed Denial of Service Attack," Working Paper, 2013.

50. Bruce Guenter, "SPAM Archive," n.d., available from *http://untroubled.org/spam*.

PART II:

CYBERSECURITY OF SMART CITIES

CHAPTER 4

CYBERSECURITY AND PRIVACY ISSUES FACING SMART CITIES: CHALLENGES AND POLICY RESPONSES

Nir Kshetri

OVERVIEW[1]

By 2050, one estimate suggests that 66 percent of the world's population, 6.3 billion people, will live in cities. The development of smart cities has been a major global trend. The global smart city market is expected to reach about $1.6 trillion in 2020. From the perspective of a smart city, an obvious and alarming trend is that cyberattacks have been capable of causing physical damage to plants and equipment. This chapter identifies and analyzes the unique challenges faced by smart cities from the privacy and cybersecurity standpoint. Since big data is a key component of smart city initiatives, this chapter examines how various characteristics of big data are linked to privacy and cybersecurity in the context of smart cities. It also compares cyberattacks targeting smart cities and other forms of cyberattacks in terms of various criteria and parameters such as seriousness of threats, likely perpetrators and their modus operandi, and possible defense responses. This chapter also reviews how privacy issues in smart cities are shaped by enduring cultural models of privacy protection and the political discourses around this issue. Also discussed are implications for policymakers, developers of smart city technologies, residents of smart cities, and consumers. Overall this chapter argues that smart cities' overreliance on digital technologies would prove to be devastating to their economic and overall welfare in the case of severe cyberattacks.

INTRODUCTION

In 2014, 54 percent of the world's population lived in urban areas, compared to 30 percent in 1950. It is estimated that the proportion will increase to 58 percent by 2025 and 66 percent (about 6.3 billion people) by 2050.[2] The development of smart cities has thus been a major global trend. While most smart city initiatives involve "smartization" of existing cities, some cities such as South Korea's New Songdo or Songdo International Business District are being built from scratch. South Korea announced its plan to build about 15 Ubiquitous Cities (U-Cities) that apply "ubiquitous computing" to integrate information systems and social systems. In 2013, China released plans for building 103 smart cities, districts, and towns. As of January 2013, over 40 Chinese municipalities had expressed plans to build smart cities. Likewise, India's Prime Minister Narendra Modi has announced plans to build 100 smart cities. Singapore, Hong Kong, Dubai, and a number of European countries have been putting together efforts and initiatives to introduce a digital city or wireless city that utilizes state of the art technology in the development of urban systems. Likewise, Japan has put in place a strategy to build a U-Japan since 2004. Unsurprisingly, the global smart city market is expected to reach $1.6 trillion in 2020.[3] As of mid-2015, South Africa had invested $7.4 billion into a smart city project.[4] IHS, a provider of global market, industry, and technical expertise uses a narrow definition of the term "smart cities" to refer to:

> cities that have deployed—or are currently piloting—the integration of information, communications and technology (ICT) solutions across three or more different functional areas of a city. . . . These functional areas include mobile and transport, energy and sustainability, physical infrastructure, governance, and safety and security.[5]

IHS concluded there were 21 smart cities in the world in 2013, which will increase to 88 or more by 2025.[6]

While Europe and Asia are ahead of the United States in implementing smart city initiatives, a number of U.S. cities have been making efforts to offer smarter, more efficient service infrastructures. Some notable examples include Boston, New York City, San Jose, San Francisco, and Seattle. New York City's $20 billion Hudson Yards project involves a 28-acre commercial and residential area. Hudson Yards will track environmental and lifestyle factors such as traffic patterns, energy consumption, and air pollution. It will also include a trash-disposal system that will remove waste via underground pneumatic tubes.[7]

Moving to the focus of this chapter, privacy and security issues are becoming key factors in consumer and business acceptance and willingness to live in smart cities.[8] In October 2013, the United Kingdom's Department of Business, Innovation & Skills noted that trust in data privacy and system integrity is a major barrier to smart city projects.[9] Experts say that there has been a lack of clear focus on cybersecurity in smart city initiatives, meaning such cities are likely to become larger and more attractive targets for cybercriminals, nation states, and cyberterrorists.[10] In 2014, a cybersecurity researcher showed that about 200,000 traffic control sensors in major hubs such as Washington, DC; New York; New Jersey; San Francisco; Seattle; Lyon; France; and Melbourne, Australia were not encrypted and thus were vulnerable to cyberattacks. The researchers demonstrated that it was possible to intercept information coming from these sensors from 1,500 feet away, or by a drone.[11]

Observers have expressed reservations about security features of the system used in smarter cities. Concerns have been voiced regarding the protection of data, systems, and infrastructures that play critical roles in the operation of the city as well as the safety and livelihood of its residents. It is argued that the challenge of cybersecurity has not been adequately addressed by smart city advocates.[12] The systems used in smart cities have sophisticated features and functionality that are often characterized as having a high degree of vulnerability to cyberattacks due to their complexity, high levels of interconnectedness, and large volume of information. The infrastructures such as broadband networks, Wi-Fi, and satellites that connect systems and operators increase the entry points for cyber-offenders.[13] If a device is successfully hacked, it may act as a pivot and bypass existing defense mechanisms. Critics have also argued that most manufacturers producing much of the devices and systems for smart cities have failed to ensure adequate cybersecurity.[14] Moreover, cyberattacks on smart cities are likely to result in more serious consequences and outcomes for the victims and higher costs to society. The emergence of malware and worms capable of causing physical damage is especially alarming and of concern, as they are likely to target smart cities. These concerns have stimulated substantial cybersecurity spending in smart cities, which according to Pike Research, is expected to reach $1.3 billion by 2015.[15]

The above problems are especially acute in developing countries that are characterized by a nascent stage of critical infrastructure protection and weak cybersecurity policies. For instance, India's national cybersecurity policy has been described as "very weak," and it had not been implemented by the Indian government even 2 years after it was made public.[16]

A related point is that residents of smart cities have found that a digital lifestyle may have significant privacy costs.[17] The analysis and integration of data streams has facilitated surveillance and "dataveillance" (tracking the trails created by a person's activities) and increased the threat of a "big brother society."[18] For instance, in South Korea's New Songdo City, which is described as the world's first greenfield smart city, a smartcard serves as a resident's personal key to do everything from riding buses and subways, to paying for parking, watching a movie, and borrowing a bicycle. The relational nature of various activities, which contain a common field, makes it possible to conjoin and combine different data sets.[19]

There are even more concerns in cities such as Addis Ababa, Cairo, and other cities with strict government cyber-control measures. In these cities, bloggers and organizers of social mobilizations have been imprisoned for criticizing their governments.[20] In 2011, the Chinese Government announced a plan to introduce an "information platform of real-time citizen movement." The stated goal of the plan was to tackle congestion by monitoring the flow of people. Human rights activists expressed concerns that the regime may use the information to suppress activists. For instance, cell phones of activists have already been allegedly tracked by security forces, which are used to locate activists and track their movements.[21] However, when compared to more democratic societies, civic societies hold positions of less power in discourse in China. For instance, Brazil's Rio de Janeiro's attempts to "smartize" the city drew concerns related to cybersecurity and privacy violations from citizens.[22]

Some argue that growing privacy concerns could act as a barrier in citizens' adoption and use of some smart city related technologies and services.[23] Some analysts also believe that new legislation may be essential to guarantee privacy in smart cities.[24] Mayors and other civic leaders are participating in developing the visions of smart cities.[25] Certain discourses have evolved in the context of privacy issues. As noted above, due to privacy and security issues, such projects have faced resistance and opposition by citizens.

Before proceeding, we offer some clarifying definitions. A smart city involves the use of technology to gather and analyze data and take actions in order to enhance efficiency and improve the quality of life.[26] "*Cyber-physical systems (CPS)* are smart systems that include engineered interacting networks of physical and computational components [italics in original]."[27] That is to say that in a CPS, physical entities can interact with and are controlled by collaborating computational elements. A CPS processes the collected information and acts. A CPS can facilitate the real-time collection and analysis of data related to diverse aspects of areas such as health, environment, energy and water usage patterns, traffic, and waste disposal, and thus is likely to play key roles in smart cities.

In this chapter, we proceed by first discussing the privacy and security challenges facing smart cities. Next, we analyze the issue of big data in smart cities from security and privacy perspectives. The final section provides discussion and implications.

PRIVACY AND SECURITY CHALLENGES FACING SMART CITIES

Major challenges that face smart cities include: securing against cyberattacks and terrorism, maintaining safety of the controlled systems, protecting intellectual property and other assets, and protecting privacy rights.[28] First, smart cities raise major privacy issues. Entities who provide services to the residents of smart cities need to have access to data in order to provide better services. CPSs thus often manage large amounts of data and information related to health, gender, religion, and other sensitive indicators.[29] In addition, a cyber-offender can also monitor events such as residents' movement patterns in a large number of buildings and create profiles that can be sold in an underground market.[30] Prior researchers have noted that there exists a substantial market for such information.[31] For instance, in China, a malicious actor can sell a database containing a specific type of information for more than $1,500 on the black market. The illegal companies, in turn, charge their clients between $1,500 and $150,000 for services such as private investigation, illegal debt collection, asset investigation, and even kidnapping.[32]

Smart cities use vehicles and people as sensors. In many cases, information is not available about the trustworthiness of the receivers. People, who are acting as sensors, may experience adverse consequences if their information is misused.[33]

A comparison of cyberattacks targeting smart cities with major forms of cybercrimes such as the Nigerian 419 fraud, click frauds on pay-per-click advertising, Denial of Service (DoS) attacks, and phishing can provide important insights to understand various aspects of such attacks. Table 4-1 compares identity thefts to cyberattacks targeting smart cities.

Some analysts have argued that, unlike nuclear weapons, cyberwar is less likely to pose an "existential threat to humanity."[34] However, a preliminary look at some cyberattacks targeting smart cities challenges this observation and indicates that cyberthreats facing smart cities can be costly and dangerous. Terrorists and adversary states can launch cyberattacks, which may pose existential threats to those living in smart cities. Buildings can also be used to blackmail the inhabitants and owners and force them to transfer their money to criminals.[35]

	Identity Thefts	Cyberattacks Targeting Smart Cities
Seriousness of Threats	• Mostly low level of seriousness.	• Low to high levels of seriousness including existential threats due partly to the emergence of malware and worms capable of causing a physical damage.
Likely Perpetrators	• Mainly financially motivated cybercriminals.[36]	• Attractive targets for cybercriminals, terrorists, and adversary governments. • As cities become smarter and more connected, financially motivated cybercriminals perceive a change in the cost/benefit calculus and target them.
Modus Operandi of Perpetrators	• Deployment of relatively older virus, malware, worms, and social engineering tools.	• Deployment of relatively newer virus, malware, and worms such as the Internet of Things (IoT) botnet and building automation systems (BAS) botnet.[37]
The Defense Responses	• To some extent, organizations and individuals have developed technological, behavioral, and cognitive defense mechanisms.	• Generally underdeveloped defense mechanisms. • Relatively little guidance regarding how to configure IoT. • Not enough attention from device makers, governments, and organizations for IoT security flaws.

Table 4-1. A Comparison of Identity Thefts to Cyberattacks Targeting Smart Cities.

In order to illustrate the previous point, this chapter reviews a number of malware products and worms that have been designed to target industrial control systems (ICS) and cause physical damages. Some examples include Stuxnet, Duqu, Flame, BlackEnergy, and Shamoon. Stuxnet, for instance, caused the centrifuges of the uranium in an Iranian nuclear facility to over-spin and self-destruct. The operator's console falsely showed that the system was operating within normal parameters and values. In another example, the Duqu malware looked for useful information to attack an ICS. Likewise, the Flame malware searched for engineering drawings, specifications, and other technical details about the systems. It also recorded audio, screenshots, keyboard activity, and network traffic. Its capability also included recording Skype conversations and turning infected computers into Bluetooth in order to download contact information from nearby Bluetooth-enabled devices.[38] Likewise, the U.S. Department of Homeland Security (DHS) identified BlackEnergy within an ICS used by critical infrastructures. A senior threat researcher at Trend Micro noted that BlackEnergy was targeting some of the ICSs that were exploited by Stuxnet.[39]

The attacks attributed to Shamoon wiped out the hard drives of 30,000 computers, 85 percent of the Armco's devices, and shut the company's business down for two weeks.[40] The costs associated with replacement and incident response were estimated to exceed $15 million.[41] Several months following the first attacks, the Shamoon malware reportedly tried to attack the oil and gas flow networks in an attempt to disrupt international supplies.[42] Shamoon demonstrated the ability to spread to other computers on the network by exploiting shared hard drives. The virus compiled a list of files from specific locations, erased them, and sent file information to the attacker.[43] According to a December 2014 report of Germany's Federal Office for Information Security, hackers caused physical damage to a facility of a steel plant. The attackers had used spear-phishing and social engineering to gain access to the plant's network, where they subsequently penetrated the production network.[44] It was reported that the attack resulted in "massive" damage.[45] This attack was the second confirmed case, after the Stuxnet attack on an Iranian nuclear facility, in which a purely cyberattack caused the physical destruction of a plant or equipment.

The privacy and security risks facing smart cities are relatively newer, less known, and rapidly emerging. For instance, a major vulnerability of smart cities relies on the fact that they are attractive targets for the IoT botnets. In the first cyberattack involving the IoT, a botnet of more than 100,000 Internet-connected devices sent over 750,000 malicious emails from December 23, 2013, to January 6, 2014.[46] If a hacker is able to break into any of the IoT devices, such as automatic doors, smart home heating and lighting systems, vending machines, cameras, security alarms, Wi-Fi router boxes, entertainment gadgets, and smart televisions (TVs), then it is easy for the hacker to gain access to broader networks (e.g., corporate networks).[47] In a discussion of the IoT, it is noted that buildings are associated with major vulnerabilities and security threats. In particular, BAS, and supervisory control and data acquisition (SCADA), which have been important choices for facilities management and building operational needs, may represent a key vulnerability factor. BAS and SCADA deployments are associated and facilitated by the need to upgrade energy infrastructures. Frost and Sullivan, the Gartner Group, and Forrester have expressed concerns regarding the cybersecurity threats of these systems.[48]

Note that BAS are "centralized, interlinked, networks of hardware and software, which monitor and control the environment in commercial, industrial, and institutional facilities."[49] One estimate suggested that there are more than 15,000 BAS in the United States that are accessible via the Internet, 9 percent of which are reported to have cybersecurity vulnerabilities.[50] Since such systems are often incorporated into computer networks, an attack on BAS makes it easy to penetrate the company network.

From the offender's standpoint, there are a number of benefits associated with developing malware to attack the systems in smart cities. BAS are permanently available, often have no security features, and are rarely patched. These features are attractive for botnet operators, cybercriminals, and insiders.[51] If a hacker successfully attacks a BAS system, it is easy to penetrate other devices and computers on the network. This is because attacks coming from inside the network are trusted and ignored by traditional network security. Therefore, employee records, customer data, and intellectual property are likely to become vulnerable to cyberattacks.[52] A cybersecurity researcher put the issue this way: "[A] simple problem can have a large impact due to interdependencies and associated chain reactions."[53] This means an adversary can launch a cyberattack on a seemingly uncritical and poorly secured system, resulting in chaos.[54]

According to a report of the U.S. DHS in April 2013, hackers targeted building energy-management systems. Companies connect building energy-management systems to networks and the Internet to automate lighting, heating, and air conditioning. Cybercriminals can use these connections to unlock doors and turn off lights. Quoting financial institutions, a security researcher noted that if the temperature is changed by 5-6 degrees, the computers could not process transactions at the normal rate.[55] Cybercriminals thus can damage data centers by turning up the heat.

In 2012, security researchers found at least two vulnerabilities in Tridium's building management software. Note that Tridium Niagara software is used in many building management systems. As of August 2012, the software was used by over 300,000 organizations in 52 countries in order to remotely control and monitor a wide range of devices and equipment such as medical devices, elevators, furnaces, video cameras, and security systems.[56] The researchers were able to exploit vulnerabilities in Tridium Niagara software to open a company's parking garage gate and the front door. They were also able to penetrate into the company's corporate network. In 2012, cyberattackers reportedly exploited Tridium vulnerabilities at least twice. In a New Jersey manufacturing company, attackers discovered the system was accessible from the Internet. In the second instance, a state government facility was attacked and the temperature settings in the building were changed.[57]

Some technologies and devices that are more prone to privacy issues are likely to be adopted in smart cities compared to conventional cities. Some examples of such systems are smart meters and smart grids. According to Pike Research, about one-third of smart city projects in North America and Europe were primarily focused on smart grids or other energy innovations, and about half of smart city strategies include energy-focused projects.[58]

Concerns over privacy and security have been an important part of the debate over the impact of smart meters and smart grids. As of the end of 2014, in the United States, 38 million smart meters were installed, which gather information about household electricity consumption and transmit to the supplier.[59] The U.S. Department of Energy announced a plan to publish a voluntary code of conduct to govern data privacy for smart meters in January 2015. Despite the existence of such code, some critics are concerned that consumers could be persuaded into giving up their private data to power companies and third-party data aggregators.

Data transmitted by smart meters are often high-value data. It is argued that the electricity consumption data is worth more than the commodity consumed to generate the data.[60] This is because many devices transfer data among themselves and generate new data, also referred to as derived data.[61] Devices connected to the smart grid thus may leave key information behind. This type of privacy is also called footprint privacy, in which transactions, actions, and queries associated with the concerned devices are stored.[62]

Such data is likely to permit more sophisticated profiling and targeting of consumer and neighborhoods that can be used for purposes such as retailers' decision to open the next store.[63] These concerns are of special interest to smart cities. It is often not clear how the data is used and who uses it. Some have also argued that cities may have to create their own privacy charters to address concerned citizens.[64]

To be useful for purposes such as increasing energy efficiency by giving consumers greater control over their use of electricity, permitting better integration of plug-in electric vehicles and renewable energy sources, developing a more reliable electricity grid to withstand cyberattacks, natural disasters, and help to decrease peak demand for electricity, data recorded by smart meters must be highly detailed.[65] For instance, it may show the types of appliances a consumer is using.[66] According to a European Union data watchdog, new energy smart meters can track whether consumers are at home or not, how they spend their free time, and the type of medical devices they use.[67] When the data is transmitted to electric utilities or stored, potential interception or theft is possible.[68] Precise and frequent measurements of utility consumption allow the collection and inference of a huge amount of confidential information, which can be used for user profiling on the basis of personal behavioral patterns.[69]

In other settings, in order to protect themselves from established cybercrime types, individuals and organizations are developing technological, behavioral, and cognitive defense mechanisms. Corporations are also facing regulatory pressures to change their business models so as to minimize real and perceived vulnerabilities. Consequently, businesses are revamping their organizational structures, and cybersecurity specialists have started holding key positions in the organizational hierarchy. An increasing number of companies are recruiting board members who emphasize the importance of cybersecurity.[70]

Defense mechanisms have been less clear to protect against cyberattacks targeting smart cities. The idea of rare enemy syndrome provides a helpful perspective for understanding how unfamiliar baits tend to achieve more success.[71] With the terms that evolutionary biologists use, it can be argued that the enemy's manipulation is so rare that the victim has not developed an effective counter poison.[72] That is, evolutionary development has not yet progressed to that point. To put things in context, observers note that cities have plans for natural disasters such as earthquakes and floods, but lack mechanisms to deal with cyber-attacks.[73]

IoT botnet and BAS botnet are a relatively new phenomenon. Hackers gain access to devices because homeowners do not set them up correctly, or use the default password that comes with the device.[74] Likewise, there is relatively little guidance regarding how to configure IoT. Device-makers, governments, and organizations have not paid enough attention to IoT security flaws.[75] A cybersecurity expert noted that the IoT devices pose complex governance and management problems from the cybersecurity standpoint, because they are designed for specific purposes instead of general-purpose computers.[76] A related problem is that securing the IoT is arguably a "moving target," since what constitutes an IoT is still evolving itself.[77] Likewise, progress to fix ICS security issues has been slow due to the poor design of existing systems and a lack of strong incentives to fix the problems. Part of the issue is that current laws do not make the manufacturers of control systems liable for poor cybersecurity.[78]

LOOKING FROM A BIG DATA PERSPECTIVE

The use of data and analytics arguably represents the latest stage in the evolution of the discussion of the issues of smart cities.[79] Big data is generated by sensors, meters, cameras, in-car navigation devices, smart phones, pollution monitoring stations, energy meters, and other devices and processes. Some organizations and governments have introduced high profile initiatives that are aimed at improving cybersecurity involving big data in smart cities. For instance, in 2014, Singapore Telecommunications Limited (Singtel) announced a plan to invest $500 million and hire 1,000 engineers over the next five years in order to build cybersecurity, smart cities, and big data analytics.[80]

The relationship of big data with privacy and security issues in smart city initiatives is presented in Table 4-2.

Volume.

Huge data volume is arguably the most important feature of smart cities. Smart cities involve surveillance and sensor technologies for city planning, incident response, traffic coordination, and crime management.[81] In such a system, there is an incentive to collect and act upon as much data as possible. For instance, the New Songdo City makes extensive use of radio-frequency identification (RFID) technology. Using RFID, public recycling bins credit every time an individual recycles a bottle.[82] Likewise, an estimate suggested that Philadelphia is saving $1 million annually from fitting garbage bins with sensors, which indicate when the bin is full, thus reducing the number of required collections.[83] Moreover, most types of data in smart cities are often fine-grained in resolution and detail, and thus are attractive targets for perpetrators. These conditions create a high degree of vulnerability to cyberthreats and privacy violations.

In a big data environment, each data point competes for attention.[84] A huge amount of data means that security breaches and privacy violations are likely to lead to more severe consequences and losses via reputational damage, legal liability, ethical harms, and other issues, which are also referred to as an "amplified technical impact."[85]

Velocity.

Smart city residents exhibit a higher degree of reliance on real-time data. For instance, smart cities collect real-time data from roads and manage traffic lights based on traffic volume.

Real-time data is also used in helping people with serious health issues. New Songdo's "U-protection" service aims to use mobile health-sensor technologies to manage health conditions of senior citizens, especially those living alone. Location-based technologies will identify elderly citizens with Alzheimer's in case they are lost or face problems.[86] Such an overreliance on real-time data may lead to calamity and severe consequences in the case of a data breach or privacy violation. A criminal can also use location data for stalking people in real-time.

Variety.

Data comes in multiple formats such as structured and unstructured. Of special concern is much of the unstructured data such as road traffic information and Binary Large Objects (BLOBs)—e.g., multimedia objects such as images, audio, and video—that are sensitive in nature and may contain personally identifiable information (PII).[87] For instance, a closed-circuit television (CCTV) network, which enables the exchange of video data generated by Seoul's 30,000 CCTV installations, is a key component of the city's telecommunication network known as U-Seoul Net.[88] According to Gartner, the security of unstructured data has been a seriously under-recognized problem.[89]

Variability.

Data in smart cities comes from a wide variety of sources. For instance in New Songdo, residential, medical, and business information systems are integrated into one system.[90] Some of the information sources may be characterized by variable rate of data flows. For instance, higher rates of business related data flows might occur during business hours.

The time-variant nature of data flows mean that privacy and security issues are of more significance during peak data traffic. Organizations may lack capabilities to securely store huge amounts of data and manage the collected data during peak data traffic. In December 2013, Target announced that its high-profile security breach, which compromised 40 million credit and debit card accounts and the personal data of 70 million people, occurred during the peak holiday shopping season from November 27 to December 15. The virus tried to steal card data during peak customer visit times (10 a.m.-5 p.m. local times) of targeted stores.[91]

Complexity.

Data in smart cities comes from a number of sources. Availability of data from multiple sources (e.g., smart meters, car sensors, trashcans) makes it easy to track residents and their actions in great and minute detail that may lead to a high degree of privacy violation and severe security problems.

Characteristic	Explanation	Collection/Storing
Volume	• Huge amount of data is created from a wide range of sources such as transactions, unstructured streaming from text, images, audio, voice, Voice over Internet Protocol (VoIP), video, TV and other media, sensor and machine-to-data.	• High data volume would likely attract a great deal of attention from cybercriminals. • Some data (e.g., transmitted by smart meters) are often high value data.
Velocity (Fast Data)	• Some data is time-sensitive for which speed is more important than volume. Data needs to be stored, processed, and analyzed quickly.	• Operating a smart city involves collecting real-time data from roads and managing traffic lights based on traffic volume. Residents exhibit a higher degree of reliance on real-time data. Such an overreliance on real-time data may lead to calamity and severe consequences in case of data breaches or privacy violation.
Variety	• Data comes in multiple formats such as structured, numeric data in traditional databases and unstructured text documents, email, video, audio, and financial transactions.	• Of special concern is much of the unstructured data that is sensitive in nature and may contain PII.
Variability	• Data flows can vary greatly with periodic peaks and troughs. These are related to social media trends, daily, seasonal, and event-triggered peak data loads and other factors.	• Cities may lack capabilities to securely store huge amounts of data and manage the collected data during peak data traffic. Attractiveness as a crime target increases during such period.
Complexity	• Data comes from multiple sources that require linking, matching, cleansing, and transforming across systems.	• Availability of data from multiple sources (e.g., smart meters, car sensors, trashcans) makes it easy to track residents and their actions in great and minute detail that may lead to a high degree of privacy violation and severe cybersecurity consequences.

Table 4-2. Big Data Characteristics in Relation to Security and Privacy in Smart Cities.[92]

DISCUSSION AND IMPLICATIONS

Some of the emerging and alarming trends discussed above indicate that cyberattacks on smart cities are likely to have dangerous consequences. Smart cities are likely to be ideal targets for cyberterrorists and hostile foreign governments. Traditional devices owned by businesses and consumers have been the most popular target for financially motivated cybercriminals. However, as cities become smarter and more connected, it is likely that such cybercriminals will perceive a change in the cost/benefit calculus and target them. Likewise, the development and deployment of directed, automated, and networked technologies have led to a surge in surveillance activities and programs. Smart city developers and policymakers thus need to make sure that privacy and security concerns are adequately addressed and clearly resolved. No less important is the implementation of measures to educate consumers so that they understand the potential value of various categories of information belonging to them. It is also important to take into account the influence of perception as well as reality in consumers' assessment of privacy and security issues.

Equally important is the need to understand the desired level of privacy of consumers. For example, an intriguing aspect of the development of South Korea's New Songdo City is that most of the core technologies were developed in the United States rather than in Korea. Supportive formal and informal institutions including lower privacy concerns are arguably the primary reason why the U.S.-developed smart city technologies were first implemented in Korea rather than anywhere else.[93] While the use of RFID to automate tracking and monitoring the movements of people is a big concern in the West, privacy concerns are less prominent in Asia.[94] As a research director of Palo Alto described, "There is an historical expectation of less privacy [in Korea]."[95] Observers have also noted that, whereas ubiquitous computing is controversial in the West due to privacy concerns and fears of turning into a surveillance society, in Korea and other Asian nations the concept is viewed as an opportunity to attract foreign investment by showing off technological prowess.[96] Ubiquitous computing is arguably viewed more as gaining technology expertise in Asia rather than an invasion of privacy.[97]

Whereas strong legal protections for the privacy of personal information exist in the European Union and clear laws exist as to how data can be collected, stored, and reused, privacy is a new luxury in most cities in Asia and other parts of the world.[98] Likewise, authoritarian regimes of the Persian Gulf view surveillance and data mining as a means to increase their power and control over terrorists, criminal outfits, minority groups, and migrant workers.[99]

With respect to privacy issues, it is important to note the existence of heterogeneous laws, views, interests, and opinions internationally. A "one size fits all" approach to the design and development of smart cities may be ill-advised and likely to be ineffective in terms of meeting the privacy needs of different groups of people. Alternative utopias of smart cities have been offered. One possibility is "a perfectly controlled, perfectly efficient, safe smart city."[100] A smart city taken over by computers designed by a big technology company is likely to function like a machine. This highly automated and highly centralized model is efficient, but may perform poorly in regards to privacy protection.[101] Such a model is more likely to work for societies in which privacy may be less of a concern, but not for others in which privacy issues are salient. Therefore, U.S. companies may benefit more from exporting their ubiquitous systems to countries that are more accepting of such technology from a privacy standpoint, such as South Korea.[102]

Finally, the politics associated with data produced by big data initiatives in smart cities needs to be analyzed in terms of the societal values. It is also important to understand whose agenda and interests are primarily served by a data gathering initiative.[103] For instance, some types of data in authoritarian regimes may be collected for spying on citizens rather than providing better services to residents. Since alternative models of smart cities exist (e.g., in terms of centralization and decentralization), there is thus the need to pursue cross-national and cross-cultural comparisons systematically in order to evaluate the fit of big data initiatives associated with a given model.

ENDNOTES - CHAPTER 4

1. An earlier version of this chapter appeared as the paper Nir Kshetri, "Cybersecurity and Privacy Issues Facing Smart Cities: Challenges and Policy Responses," Presented at The City University of New York (CUNY), City College, Cyber Infrastructure Protection (CIP) Conference in New York on October 15, 2015.

2. Alessandro Zanni, "Cyber-physical systems and smart cities: Learn how smart devices, sensors, and actuators are advancing Internet of Things implementations," April 20, 2015, available from *https://www.ibm.com/developerworks/library/ba-cyber-physical-systems-and-smart-cities-iot/*.

3. "Global Smart Cities Market to Reach US$1.56 Trillion by 2020," *Transmission & Distribution World*, December 7, 2014, available from *https://ww2.frost.com/news/press-releases/frost-sullivan-global-smart-cities-market-reach-us156-trillion-2020/*.

4. Nicole Perlroth, "Security Researchers Start Effort to Protect 'Smart' Cities," Bits blog of *The New York Times*, May 26, 2015, available from *bits.blogs.nytimes.com/2015/05/26/security-researchers-start-effort-to-protect-smart-cities/?_r=0.*

5. IHS, "Smart Cities to Rise Fourfold in Number from 2013 to 2025," IHS News Release, July 29, 2014, available from *press.ihs.com/press-release/design-supply-chain-media/smart-cities-rise-fourfold-number-2013-2025.*

6. *Ibid*.

7. Michelle Reis, "5 U.S. Cities Using Technology To Become Smart And Connected," August 15, 2014, available from *www.forbes.com/sites/ptc/2014/08/15/5-u-s-cities-using-technology-to-become-smart-and-connected/#20fce0e35391.*

8. Andrea Bartoli, Juan Hernández-Serrano, Miguel Soriano, Mischa Dohler, Apostolos Kountouris, and Dominique Barthel, "Security and Privacy in your Smart City," *Smart Cities Council White Paper*, September 6, 2011, available from *smartcitiescouncil.com/resources/security-and-privacy-your-smart-city.*

9. Malcolm Dowden, "UK: Smart Cities: The End Of Privacy Or The Key To Active Citizenship?" Mondaq: Connecting Knowledge & People, March 13, 2014, available from *www.mondaq.com/x/299362/Data+Protection+Privacy/Smart+Cities+The+End+Of+Privacy+Or+The+Key+To+Active+Citizenship*.

10. Perlroth, "Security Researchers Start Effort to Protect 'Smart' Cities."

11. Nicole Perlroth, "Smart City Technology May Be Vulnerable to Hackers," Bits blog of *The New York Times*, April 21, 2015, available from *bits.blogs.nytimes.com/2015/04/21/smart-city-technology-may-be-vulnerable-to-hackers/?_r=0.*

12. Eric Woods, "Smart Cities and Big Data: Challenges and Opportunities," European Utility Week website, 2014, available from *2014.european-utility-week.com/SmartCitiesandBigData*.

13. Giampiero Nanni, “Transformational ‘Smart Cities’: cyber security and resilience,” *Executive Report: Smart Cities*, Mountain View, CA: Symantec, 2013.

14. Bartoli *et al.,* “Security and Privacy in your Smart City”; Tom Brewster, “Smart or stupid: will our cities of the future be easier to hack?” *The Guardian*, May 21, 2014, available from *www.theguardian.com/cities/2014/may/21/smart-cities-future-stupid-hack-terrorism-watchdogs.*

15. Indu B. Singh and Joseph N. Pelton, “Securing the Cyber City of the Future,” Futurist, Vol. 47, Iss. 6, November 2013, pp. 22-27.

16. Perry4Law Techno-Legal Base, “Smart Cities Cyber Security In India: The Problems And Solutions,” International Legal Issues Of Cyber Attacks, Cyber Terrorism, Cyber Espionage, Cyber Warfare And Cyber Crimes: International And Indian Legal Issues Of Cyber Security blog, May 29, 2015, available from *perry4law.co.in/cyber_security/?p=77.*

17. Nir Kshetri, Lailani L. Alcantara, and Yonghoon Park, “Development of a Smart City and its Adoption and Acceptance: the Case of New Songdo,” *Communications & Strategies*, Vol. 96, 4th Qtr. 2014, pp. 113-128.

18. Rob Kitchin, “The Real-Time City? Big Data and Smart Urbanism,” Paper presented at the Smart Urbanism: Utopian Vision or False Dawn workshop at the University of Durham, July 20-21, 2013, available from *dx.doi.org/10.2139/ssrn.2289141*; for the revised paper see Rob Kitchin, “The real-time city? Big data and smart urbanism,” GeoJournal, Vol. 79, Iss. 1, February 2014, pp. 1–14, available from *link.springer.com/article/10.1007/s10708-013-9516-8.*

19. Kitchin, “The real-time city?” February 2014.

20. Jonathan Silver, “The rise of Afro-Smart cities should be viewed with caution,” Africa at LSE: LSE’s engagement in Africa blog, July 16, 2014, available from *blogs.lse.ac.uk/africaatlse/2014/07/16/the-rise-of-afro-smart-cities-should-be-viewed-with-caution/.*

21. Tania Branigan, "China plans to track Beijing citizens through their mobiles," *The Guardian*, March 4, 2011, available from *www.theguardian.com/world/2011/mar/04/china-tracking-beijing-citizens-mobiles.*

22. MIT TR eds., "A Closer Look at Smart Cities," *MIT Technology Review*, November 18, 2014, available from *www.technologyreview.com/news/532526/a-closer-look-at-smart-cities/.*

23. Francesco Ferrero, "Privacy in the Era of Smart Cities," BVEX: Business Value Exchange, September 20, 2013, available from *businessvalueexchange.com/blog/2013/09/20/privacy-era-smart-cities/;* Antoni Martinez-Balleste, Pablo A. Perez-Martinez, and Agusti Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," IEEE Communications Magazine, Vol. 51, Iss. 6, June 2013, available from *ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6525606.*

24. Ferrero; Martinez-Balleste, Perez-Martinez, and Solanas.

25. Nate Berg, "Smart Cities Will Take Many Forms," MIT Technology Review, November 18, 2014, available from *www.technologyreview.com/news/532496/smart-cities-will-take-many-forms/.*

26. Brian Kennedy, "NIST Tackles Cybersecurity in the Smart City," Hogan Lovells Chronicle of Data Protection, June 22, 2015, available from *www.hldataprotection.com/2015/06/articles/consumer-privacy/nist-tackles-cybersecurity-in-the-smart-city/.*

27. Cyber Physical Systems (CPS) Public Working Group, "DRAFT: Framework for Cyber-Physical Systems," Release 0.8, n.p., September 2015, p. xii, available from *https://pages.nist.gov/cpspwg/library/.*

28. Radu Popescu-Zeletin, "Cyber physical systems and Smart cities," Fraunhofer: Fokus, 2015; Singh and Pelton, pp. 22-27.

29. Zanni.

30. Steffen Wendzel, Viviane Zwanger, Michael Meier, and Sebastian Szlósarczyk, "Envisioning Smart Building Botnets," in Stefan Katzenbeisser, Volkmar Lotz, and Edgar Weippl, eds., *Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit 19-21. März*

2014 in Wien (Security 2014: Security, Protection and Reliability March 19-21, 2014, in Vienna), Lecture Notes in Informatics (LNI)—Proceedings, Vol. P-228, Bonn, DE: Gesellschaft für Informatik, 2014.

31. Nir Kshetri, "China's Data Privacy Regulations: A Tricky Trade-Off between ICT's Productive Utilization and Cyber-Control," *IEEE Security & Privacy*, Vol. 12, Iss. 4, July-August 2014, pp. 38-45.

32. Zhang Yan, "Personal data crimes set to be defined," *China Daily*, July 4, 2012, available from *usa.chinadaily.com.cn/china/2012-07/04/content_15546506.htm*.

33. Scott Cadzow, "Privacy and Security in smart cities The i-Tour contribution to protecting the citizen," Cadzow Communications Consulting Limited (C3L), 2013.

34. Joseph S. Nye, Jr., "From bombs to bytes: Can our nuclear history inform our cyber future?" Bulletin of the Atomic Scientists, Vol. 69, Iss. 5, 2013, pp. 8-14.

35. Wendzel *et al.*

36. Nir Kshetri, "The Economics of Mobile Cybercrime," The 2nd Economic Research Forum, Ulaanbaatar, Mongolia, July 2-3, 2013.

37. Brad Witter, "The Move Beyond Building Automation Systems to a More Secure Energy Infrastructure," Area Development, Fall 2013, available from *www.areadevelopment.com/AssetManagement/Q4-2013/secure-facility-energy-management-systems-22627256.shtml.*

38. Michael Chipley, "Cybersecurity," Whole Building Design Guide, September 27, 2016, updated March 27, 2017, available from *www.wbdg.org/resources/cybersecurity.php?r=secure_safe*.

39. Aaron Ernst, "Is this the future of cyberwarfare? Experts warn that new malware called BlackEnergy could be used to sabotage America's most critical infrastructure," Aljazeera America, February 5, 2015, available from *america.aljazeera.com/watch/shows/america-tonight/articles/2015/2/5/blackenergy-malware-cyberwarfare.html*.

40. Ellen Knickmeyer, "After Cyberattacks, Saudi Steps Up Online Security," Middle East Real Time, August 26, 2013, available from *blogs.wsj.com/middleeast/2013/08/26/after-cyberattacks-saudi-steps-up-online-security/*.

41. Jeffrey Carr, "Why Wasn't Saudi Aramco's Oil Production Targeted?" Digital Dao: Evolving Hostilities in the Global Cyber Commons blog, updated September 14, 2012, available from *jeffreycarr.blogspot.de/2012/09/why-wasnt-saudi-aramcos-oil-production.html*.

42. Alexander Cornwell, "Cyber attacks an increasing threat for Mideast oil and gas," Gulf News, October 16, 2014, available from *gulfnews.com/business/oil-gas/cyber-attacks-an-increasing-threat-for-mideast-oil-and-gas-1.1399982*.

43. Chipley.

44. Eduard Kovacs, "Cyberattack on German Steel Plant Caused Significant Damage: Report," Security Week, December 18, 2014, available from *www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report*.

45. Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired,* January 8, 2015, available from *www.wired.com/2015/01/german-steel-mill-hack-destruction/*.

46. Greg Dixon, "What the beep!?" *The New Zealand Herald*, June 21, 2014.

47. Steve Ranger, "Internet of Things: A security threat to business by the backdoor?" ZDNet, January 27, 2015, available from *www.zdnet.com/article/internet-of-things-a-security-threat-to-business-by-the-backdoor/*.

48. Witter.

49. "Understanding Building Automation and Control Systems," KMC Controls, 2012, available from *www.kmccontrols.com.hk/products/Understanding_Building_Automation_and_Control_Systems.html*.

50. Darlene Storm, "Botnets coming soon to a smart home or automated building near you," *Computer World*, June 4, 2014, available from *www.computerworld.com/article/2476386/cybercrime-hacking/botnets-coming-soon-to-a-smart-home-or-automated-building-near-you.html*.

51. Wendzel *et al*.

52. Marc Petock, "Cyber Threats: Gone are the days of 'security through obscurity'," AutomatedBuildings.com, March 2013, available from *automatedbuildings.com/news/mar13/articles/lynxspring/130218033505lynxspring.html*.

53. Pierluigi Paganini, "Smart city systems could become a nightmare for security," Security Affairs, April 21, 2015, available from *securityaffairs.co/wordpress/36144/hacking/smart-city-systems-hacking.html*.

54. Sara Peters, "Smart Cities' 4 Biggest Security Challenges," Dark Reading, July 1, 2015, available from *www.darkreading.com/vulnerabilities---threats/smart-cities-4-biggest-security-challenges/d/d-id/1321121*.

55. Rachael King, "Cyber Attackers Target Building Management Systems," *The Wall Street Journal*, April 5, 2013, available from *blogs.wsj.com/cio/2013/04/05/cyber-attackers-target-building-management-systems/*.

56. Robert O'Harrow Jr., "Tridium issues fixes for online control system," *The Washington Post*, August 15, 2012, available from *www.washingtonpost.com/investigations/tridium-issues-fixes-for-online-control-system/2012/08/15/678ea3c2-e6e8-11e1-936a-b801f1abab19_story.html*.

57. King.

58. Eric Woods, "Why Smart Cities Need Smart Grids," Navigant Research blog, March 8, 2013, available from *www.navigantresearch.com/blog/why-smart-cities-need-smart-grids*.

59. David Perera, "Smart grid powers up privacy worries," *Politico*, January 1, 2015, available from *www.politico.com/story/2015/01/energy-electricity-data-use-113901.html*.

60. *Ibid*.

61. Kitchin, "The real-time city?" 2014.

62. Martinez-Balleste, Perez-Martinez, and Solanas.

63. Perera.

64. Woods, "Smart Cities and Big Data: Challenges and Opportunities."

65. Brandon J. Murrill, Edward C. Liu, and Richard M. Thompson II, *Congressional Research Service Report to Congress: Smart Meter Data: Privacy and Cybersecurity*, Washington, DC: U.S. Library of Congress, Congressional Research Service, February 3, 2012.

66. The Smart Grid Interoperability Panel (SGIP) and Smart Grid Cybersecurity Committee (SGCC), *Guidelines for Smart Grid Cyber Security: Volume 2: Privacy and the Smart Grid*, NISTIR 7628, Rev. 1, Gaithersburg, MD: National Institute of Standards and Technology, U.S. Department of Commerce, September 2014, available from *dx.doi.org/10.6028/NIST.IR.7628r1*.

67. "Warning over smart meters privacy risk," BBC News, June 12, 2012, available from *www.bbc.com/news/technology-18407340*.

68. SGIP and SGCC, *Guidelines for Smart Grid Cyber Security: Volume 2*.

69. David Rebollo-Monedero, Andrea Bartoli, Juan Hernández-Serrano, Jordi Forné, and Miguel Soriano, "Reconciling privacy and efficient utility management in smart cities, Transactions on emerging telecommunications technologies," Emerging Telecommunications Technologies, Vol. 25, Iss. 1, January 2014, first published September 24, 2013, pp. 94–108.

70. "PwC's Global Information Security Survey 2015 - Japanese companies are behind the global standard," Press Release, PricewaterhouseCoopers, 2014.

71. Richard Dawkins, *The Extended Phenotype: The Long Reach of the Gene*, New York: Oxford University Press, 1982.

72. W. Martin de Jong, "Manipulative tactics in budgetary games: The art and craft of getting the money you don't deserve," *Knowledge, Technology & Policy*, Vol. 14, Iss. 1, March 2001, pp. 50–66.

73. Nicole Kobie, "Why smart cities need to get wise to security – and fast," *The Guardian*, May 13, 2015, available from *https://www.theguardian.com/technology/2015/may/13/smart-cities-internet-things-security-cesar-cerrudo-ioactive-labs*.

74. Julie Bort, "For The First Time, Hackers Have Used A Refrigerator To Attack Businesses," *Business Insider*, January 16, 2014, available from *www.businessinsider.com/hackers-use-a-refridgerator-to-attack-businesses-2014-1*.

75. Joe Stanganelli, "They Want Your Enterprise Brains: Night of the Botnet of Things," Enterprise Networking Planet, October 31, 2013, available from *www.enterprisenetworkingplanet.com/netsecur/when-smart-devices-attack-the-botnet-of-things.html*.

76. BW Online Bureau, "Internet of Things will change cyber security forever: Gartner," BW Smart Cities, September 4, 2015, available from *bwsmartcities.businessworld.in/article/Internet-of-Things-will-change-cyber-security-forever-Gartner/04-09-2015-96323/*.

77. *Ibid*.

78. Tom Simonite, "Hacking Industrial Systems Turns Out to Be Easy," *MIT Technology Review*, August 1, 2013, available from *www.technologyreview.com/news/517731/hacking-industrial-systems-turns-out-to-be-easy/*.

79. Shane Mitchell, Nicola Villa, Martin Stewart-Weeks, and Anne Lange, "The Internet of Everything for Cities: Connecting

People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities," Cisco Systems Inc., 2013, available from *www.cisco.com/c/dam/en_us/about/ac79/docs/ps/motm/IoE-Smart-City_PoV.pdf.*

80. Grace Chng, "SingTel to invest $500m in cyber security, smart cities and data analytics," The Straits Times, September 24, 2014, available from *business.asiaone.com/news/singtel-invest-500m-cyber-security-smart-cities-and-data-analytics*.

81. Mike Kavis, "The Internet Of Things Is A Cybercriminals Dream Come True," *Forbes*, January 16, 2015, available from *www.forbes.com/sites/mikekavis/2015/01/16/the-internet-of-things-is-a-cybercriminals-dream-come-true/.*

82. Régine Debatty, "Korea's U-city," We Make Money Not Art, October 5, 2005, available from *we-make-money-not-art.com/archives/2005/10/public-recyclin.php*.

83. Sam Pudwell, "Smart cities and big data: Is there a limit to what we should know?" IT ProPortal, September 25, 2014, available from *www.itproportal.com/2014/09/25/smart-cities-and-big-data-is-there-a-limit-to-what-we-should-know/.*

84. Emma Stewart, "A truly smart city is more than sensors, big data and an all-seeing internet," *The Guardian*, November 21, 2014, available from *www.theguardian.com/sustainable-business/2014/nov/21/smart-city-sensors-big-data-internet*.

85. ISACA, "Generating Value From Big Data Analytics," *White Paper*, Rolling Meadows, IL: ISACA, January 2014, available from *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Generating-Value-From-Big-Data-Analytics.aspx*.

86. Rachel Keeton, "New Songdo City: City in a Box," Tegenlicht, November 1, 2013, available from *tegenlicht.vpro.nl/nieuws/inti/New-Songdo.html*.

87. Nir Kshetri, "Big data's impact on privacy, security and consumer welfare," *Telecommunications Policy*, Vol. 38, Iss. 11, December 2014, pp. 1134-1145; Catherine Truxillo, "Five myths about

unstructured data and five good reasons you should be analyzing it," SAS Learning Post, July 8, 2013, available from *blogs.sas.com/content/sastraining/2013/07/08/five-myths-about-unstructured-data-and-five-good-reasons-you-should-be-analyzing-it/*.

88. Jong-Sung Hwang and Young Han Choe, "Smart cities Seoul: a case study," *ITU-T Technology Watch Report*, Geneva, CH: International Telecommunications Union, February 2013.

89. Jeffrey Wheatman, "Six steps for securing unstructured data," CIO From IDG, August 23, 2012, available from *www.cio.co.uk/it-strategy/six-steps-for-securing-unstructured-data-3431940/*.

90. ICON, "Tech Capitals of the World," The Age, June 18, 2007, available from *www.theage.com.au/news/technology/tech-capitals-of-the-world/2007/06/16/1181414598292.html?page=fullpage#contentSwap2*.

91. Danny Yadron, "Target Hackers Wrote Partly in Russian, Displayed High Skill, Report Finds," *The Wall Street Journal*, January 16, 2014, available from *online.wsj.com/news/articles/SB10001424052702304419104579324902602426862*.

92. Kshetri, "Big data's impact on privacy, security and consumer welfare."

93. Kshetri *et al*., "Development of a Smart City and its Adoption and Acceptance."

94. Victor Rozek, "As I See It: The Digital Life," The Four Hundred: iSeries and AS/400 Insight, Newsletter, Vol. 16, No. 10, March 12, 2007.

95. Debatty.

96. Pamela Licalzi O'Connell, "Korea's High-Tech Utopia, Where Everything Is Observed," *The New York Times*, October 5, 2005, available from *www.nytimes.com/2005/10/05/technology/techspecial/05oconnell.html?pagewanted=all*.

97. Nuno Koglek, "PRISM, Big Brother and the City of Songdo," Utopicus blog, June 2013, available from *utopicus2013.blogspot.com/2013/06/prism-big-brother-and-city-of-songdo.html*.

98. Anthony M. Townsend, "Your city is spying on you: From iPhones to cameras, you are being watched right now," Salon, October 13, 2013, pp. 2-13, available from *www.salon.com/2013/10/13/your_city_is_spying_on_you_from_iphones_to_cameras_you_are_being_watched_right_now/*.

99. *Ibid*.

100. Berg.

101. *Ibid*.

102. Associated Press (AP), "South Korean city to test limits of digital development, privacy," *The Boston Globe*, November 24, 2006, available from *archive.boston.com/business/technology/articles/2006/11/24/south_korean_city_to_test_limits_of_digital_development_privacy/*.

103. Kitchin, "The real-time city?" February 2014.

CHAPTER 5

SMARTER CITIES DEMAND SMARTER SECURITY

Adel S. Elmaghraby and Michael Losavio

INTRODUCTION[1]

Smart cities and the Internet of Things (IoT) inextricably weave networked computation into the lives of billions. They thus become woven into the political life of the city. Yet there seems a blithe indifference to the security implications for the daily, mundane affairs of people. We examine how things might go wrong, how things might be righted, and the questions of accountability needed in this human system of computation. A smarter perspective on what affects security in this new information paradigm is needed.

Concerns about increased urbanization are a driving force for exploration of smarter approaches to efficient management of urban areas, leading to many smart city initiatives. With the evolution of smart cities, novel concerns related to safety, security, and privacy emerge.[2]

According to Ivan Berger:

> Some 4 billion people live in cities now, and more than 6 billion—at least two thirds of the world's population—will live in urban areas by 2050, according to the United Nations [UN]. To deal with the challenges that brings, cities will need sophisticated technologies to monitor, analyze, and quickly respond to traffic tie-ups, citizen complaints, and lots more. And they must do so in the face of budgetary constraints and other obstacles.[3]

Lee, Hancock, and Hu have provided a framework to analyze the lessons learned from smart cities such as Seoul and San Francisco.[4] In their study, they concluded that eight stylized factors are the basis of a smart city. An adapted version of these findings can be represented by only the following five factors:

1. Intelligent data collection through sensors and multiple sources;
2. Open data initiatives to engage citizens in innovation and data usage;
3. Creation of a diversified development and service sources;
4. Accelerated adoption of technology through public initiatives and incentives; and,
5. An overarching strategy needed to assure the integration and growth of a smart city.

CONVENIENCE, SECURITY, AND PRIVACY

New lifestyles may demand convenience in many aspects of daily life. No one is willing to tolerate limited access to services or demanding physical access to business or government offices when the service can be delivered over the Internet. This places increased demands on such offices to open up their systems to the users. Convenient access to such services is in many ways the reason for the increased vulnerability of data leading to security and privacy challenges. Figure 5-1 shows that smart cities are mainly focused on providing convenience and are founded on security and privacy.

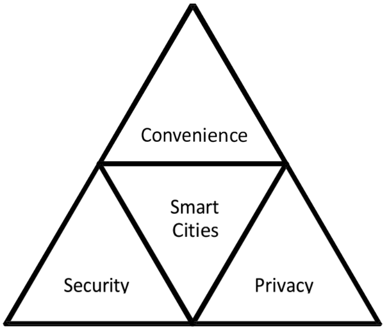


Figure 5-1. Convenience, Security, and Privacy.

CONNECTED INFRASTRUCTURE

Technological advances in the office, home, transportation, and service industries are the foundations of a smart city. Cesar Cerrudo has studied issues such as hacking traffic controls and other vulnerabilities.[5] He identified a list of technologies that help cities become smarter, and the technologies that are required on the back-end to support them.

In an earlier work,[6] the present authors identified the components of smart cities as a whole domain comprised of sets and relations.

The sets are mainly: the Persons (P), the Servers (S), and the Things (T) that are elements of the IoT. Essentially, we have:

$$\mathrm{P} = \{p_1, p_2, \ldots, p_L\}$$
$$\mathrm{S} = \{s_1, s_2, \ldots, s_M\}$$
$$\mathrm{T} = \{t_1, t_2, \ldots, t_N\}$$

Where $\mathrm{M} < \mathrm{L} \ll \mathrm{NM} < \mathrm{L} \ll \mathrm{N}$ since the number of servers and trusted entities are by far much less than the number of persons and clearly much less than the devices comprising the IoT, which is the backbone of smart cities. In addition, traditionally, the focus of attacks has been on servers; therefore, most security efforts have focused on securing servers. With the explosion of interaction between people and devices, the trend started to shift toward that communication link. However, with the next steps already in place, we project that the interaction among things is the next frontier of security and privacy.

A SMART SECURITY REGIME

How bad can it be? We have argued that an effective information security regime must begin to incorporate lessons learned for public security in the non-cyber realm. The U.S. Director of National Intelligence has promoted the idea that "Changing the Game" is the only way to re-revitalize an effective information security regime for our information infrastructure. Yet changing how we approach security, as with every change of paradigm, has been difficult. Cybersecurity reports have detailed the vulnerabilities in home, consumer, and small business systems that in turn, may serve as attack platforms against other systems. However, little has been done in this domain except by operating system designers who incrementally add protections without full involvement of the users at risk. This becomes a huge mash-up with the smart city and the IoT. The integration of computational elements into all aspects of life requires examination of information security as public security. It requires engagement at all levels of the information polity, from high-level designers to the user on the street and in their homes.

For the smart city, this is directly connected to the protection of the governmental infrastructure using computational technologies to enhance service and efficiency. Compromise of those systems, so fundamental to daily life, could crash the social ecology that the smart city seeks to support. With the IoT, this moves into direct and immediate personal security for individuals within the computational social ecology. Each personal device can represent an opportunity for enhanced well-being and a vector for attack.

Attacking the Smart City.

Cerrudo detailed the diversity of interconnected applications within the smart city, and a sampling of the vulnerabilities to those systems reads like a traditional list of information security issues:

- Lack of Cybersecurity Testing
- Poor or Nonexistent Security (implementation)
- Encryption Issues (poor or nonexistent implementation of)
- Lack of Computer Emergency Response Teams (CERTS)
- Large and Complex Attack Surfaces (a target rich environment)
- Patch Deployment Issues
- Insecure Legacy Systems
- Simple Bugs with Huge Impact
- Public Sector Issues
- Lack of Cyberattack Emergency Plans
- Susceptibility to Denial of Service (DoS)
- Technology Vendors Who Impede Security Research (in order to protect their proprietary market position)[7]

All of these represent standard issues for information security and corporate governance: lack of knowledge, money, and foresight.

Cerrudo also details various "wide-open" city-cyber infrastructure security failures with examples of potential damage from intentional compromise. He then notes the proof of concept exercise compromising the traffic control systems due to a lack of communication encryption. This could potentially affect 100,000 intersections in the United States and Canada.[8] Critically, he notes that there is no way to assure remedies for such vulnerabilities. He notes this is not simply a matter related to criminality, but one that opens a target rich environment for war fighting over the wire.

A core concern is the nature of political accountability, which often acts in a post hoc, retrospective manner after a failure of government. Public accolades and positive press coverage come with the deployment of new smart technologies for the city. However, who will be held accountable for the failure of those systems? Moreover, particularly with the lagging nature of political accountability, were only those who are currently in office held responsible for failures that may have predated their tenure, how will the expenditure of monies to security systems be viewed by the taxed public?

Attacking the Citizens of the Smart City.

The ubiquitous deployment of interconnected computable systems will, as with the smart city, offer expanded conveniences and efficiencies for personal life. Yet, each such system can offer a personal vector to attack an individual.

One historical example of this phenomenon deals with online and electronic payment systems, which have become the focus of theft activities by criminals. As the use of these systems has exploded, so has exploitation. The technical information security-based response to the problem of static credit card encoding information being duplicated and forged was the new Europay, Mastercard, and Visa (EMV) chips for credit cards that dynamically assigned transaction information that, once used, could not be reused for further transactions. This has drastically reduced counterfeit credit card fraud in Europe. While this same benefit may be expected for in-store credit card use in the United States, it will also produce a shift toward online transactions (which will not have the same level of security) and check counterfeiting. It may also increase the impetus for credit card theft and the commensurate personal risk this may entail.

We posit that this will begin to be seen across domains involving devices throughout people's lives. Health, transportation, social engagement, entertainment, and work: all of these domains may be instrumented and exploited.

Attacking the Smart Citizens of the Smart City.

This is a consequence of the interactive nature of the smart systems we hope to introduce into our lives. Think of the mischief. Think of the misery. Therefore, as in other aspects of our lives, **people** need to be prepared for their own guardian roles in the safe deployment of these technologies throughout our world. The understanding of interaction among various elements of information exchange is mandatory. In Figure 5-2, some of the nodes involved in such information exchange are highlighted.

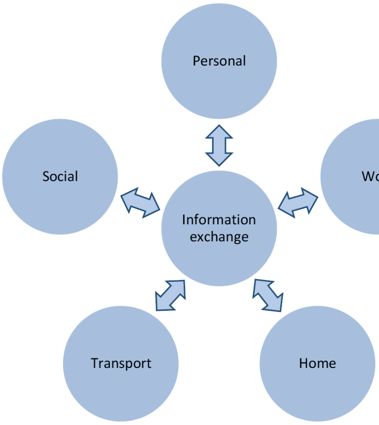


Figure 5-2. Exchange Nodes of Activities and Services.

We look at these vulnerabilities and map them to standard crimes that, in the past, required a physical presence and risk for the perpetrator.

1. Murder, Aggravated Assault.

Causing the death or physical injury of another, absent justification, is a crime in all systems of criminal law. Simple elements are the act that causes death or injury, the intent to commit that act, and the resulting death or injury. The highest penalty is for a death that was intended and accomplished.

One of the first proof of concepts relating to the use of instrumented and interconnected devices was that of the hacked operating system for a personal insulin pump via its Bluetooth port. Demonstrated by Jay Radcliffe at the 2013 Black Hat conference, one commentator observed that the more disturbing aspects of this were the significant lack of both security controls and incentives for manufacturers to properly secure their systems.[9]

More recently, security researchers Charlie Miller and Chris Valasek demonstrated the control takeover of a 2014 Jeep Cherokee, shutting off the engine, disabling the brakes, and turning the steering wheel.[10] Given the number of deaths caused by defective floor mat/accelerator combinations and effective ignition switches causing some airbags to fail during crashes, the murder and mayhem that would follow from this kind of attack could be significant.

The motives for such actions are the same as with any other crimes of violence. Jealousy, envy, and hatred, all of which play a role in criminal conduct, can now be enhanced through the use of these new technological tools.

2. Assault, Stalking, Harassment, Sexual Assault, Invasion of Privacy.

Stalking and harassment were given new extensions with the development of information technologies and the Internet. Facebook page harassment, use of systems to track people, and text messages or emails with vile content have all been used in this context.

However, the intensive penetration of our lives by more technology creates even more opportunities. Invasive monitoring of webcams unbeknownst to a homeowner, or the placement of hidden webcams can radically change the dimensions of voyeurism. The ability to capture extensive video and then to publish it online around the world deeply expands the damage done by such conduct.

At the other end of the spectrum are new opportunities for malicious mischief and vandalism, simply inflicting misery on others because it can be done. Much of this kind of malicious behavior, representing some of the earliest illegal behavior with the dawn of the Internet, can now find its way into all manner of small torments. The kitchen, for example, offers a host of opportunities. The Internet toaster can now always burn the toast. The Internet refrigerator can defrost or spoil a week's worth of food. The Internet stove can be manipulated to ruin breakfast, lunch, and dinner. Security and practices are needed to prevent this.

3. Burglary, Theft.

Lastly, we have to consider the way that the physical security systems of our families, homes, transportation, and businesses might be configured within this interconnected environment. Should we rely on these electronic security systems, which seem to offer so much? If so, we may also face a common vulnerability base that may allow physical injury in all spaces and the theft of the things within them. Indeed, used with the monitoring systems themselves, it may inform the criminals both of the goods available and the location of the people who might otherwise complicate a theft and deter its execution, or themselves become targets of physical attack.

Fighting the Attacks: Application of Criminological Theory.

We look at these vulnerabilities to give body to the problems faced by these new and amazing systems that do not consider security as a primary function simply because that is not the designers' forte. These new systems are meant to do something good, and the exploitation of them by bad people is an afterthought. Given the expanse of these vulnerabilities, and how it may allow for an expansion of those vulnerabilities to affect our own physical safety, we need to integrate security and security practices now, as we have done with the traditional aspects of our lives.

It is valuable to look at the application of modern criminological theory in this technical space. These theories help identify potential perpetrators. However, they can also help identify vulnerabilities in the human factor and ways in which systems may be best configured to reduce exploitation. Whether it is general strain theory, social control theory, routine activities theory, or other theoretical models that define the space for criminal conduct and public security, these models should be examined and mapped into the conduct that will be beneficial in both the smart city and the IoT, and identify potential risk from those that will harm others.

Routine Activity Theory posits the benefits of both a suitable guardian and the hardening of an available target. These can be strengthened by practices shifted to the private and public realms, just as the IoT/smart cities paradigm shifts to these realms. Strain Theory examines elements that both heighten the risk of deviant behavior (particularly insiders), as well as the risk of victimization (either individually or as a member of an organization opening a door to an attacker). Social Control Theory examines related and complementary factors that, again, can have an impact both on deviant attacks and the heightened risk of victimization. Displacement theory addresses how the "hardening" of one class of potential targets/victims may simply lead to victimization of other targets, a special concern for the target-rich environment of technologically advanced polities like the smart city.

These and other aspects of criminology may take these information security issues and map them to programs that have successfully reduced crime and victimization in the traditional world. They may serve as models for enhanced security within the smart city and the IoT in private life. These do presuppose a general security regime in place on core systems, itself questionable in some political environments.

Possible Responses: Initiatives that Reflect New Practices.

New possibilities for effective responses in public/information security can be seen in two initiatives by a global nongovernmental organization (NGO) that focuses on worldwide economic prosperity and security. These examples, initiatives of the World Economic Forum (WEF), demonstrate both the imaginative possibilities for new and effective systems of security as well as critical importance of this for the economic health of the world's economies. Conversely, failure of such an information security regime has the potential for economic damage and concurrent misery for the targeted populations.

Cyber-Hygiene.

People build wealth, but in the cyber realm, individuals are vulnerabilities for the total system. Smart cities will depend on smart systems, and smart systems will depend on informed formulation, responsive management, and efficient implementation. This applies to public safety systems, education systems, and, increasingly, information and communication technology (ICT) systems. In fact, the "smarter" cities get, the more ICT systems, through the Internet, will insert themselves into other systems. As the IoT becomes more ubiquitous, the safety of not only ICT systems, but also every system that has any kind of connectedness to the web will be in doubt. These are the fears of every large organization, from governments to corporations. Many of these organizations have decided the best way to protect themselves proactively is to institute cyber-hygiene regimes by creating and implementing Critical Controls.

Cyber-hygiene can be most clearly explained by analogizing it to another critical system for cities: public health. While the public becomes glued to television (TV) coverage of outbreaks of frightening diseases like the plague or Ebola, a vastly larger number are killed every year by more outbreaks of mundane diseases like malaria or influenza. Straightforward solutions that are now thought of as simple, such as washing hands or covering the mouth when coughing, can prevent the spread of these diseases and eliminate a huge amount of risk, allowing resources to be focused on larger, more complex threats. Cyber-hygiene works in much the same way—preventative measures can be can be taken to mitigate the thousands of everyday low-level attacks that cause the vast majority of security issues so that resources can be focused on larger, more dangerous threats. These measures are known as critical controls, a set of actions that are the most important things to do first when trying to reduce vulnerability and ensure sound cyber-defense. This is especially important in the era of the IoT, where everything from cars to insulin pumps to lightbulbs are fitted with microchips and connected to the web. Technological advances have outpaced their ability to be secured, and with ever-increasing hyper-connectedness, there are more fronts than ever before on which to attack. More complicated linkages between endpoints and central databases have led to attacks in areas previously thought safe, or at the very least, unnecessary to closely guard. The 2015 hacking of a Jeep Cherokee proved that linkages in the IoT could be its downfall when hackers entered the car's computer through its entertainment system and then gained control of steering and braking functions. This is why a cyber-hygiene system is so critical to ensure well-run, cyber-secure smart cities.

Several organizations, including the SANS Technology Institute and the Council on Cyber Security, have created their own set of Critical Security Controls. The challenge, though, is the implementation of popular security measures across populations and groups, not just by expert organizations.

Cyber Resilience.

Another initiative that reflects this is the cyber resilience effort of the WEF, which, again, is concerned with global economic policy that recognizes the critical nature of cybersecurity in that economy. It argues for the need for an integrated approach.[11] This recognizes the reality of information security: it will never be perfectly secure, no more than banks or levees, and recovery planning and execution are essential.

The WEF recommendations in this space are for the private sector, public sector, their collaborative intersection, and the academy. They include, even at this late date, true awareness, best practices implementation, criminal justice engagement, trans-jurisdictional collaboration, and continued research on incentive factors. As detailed in its policy statements, they cover:

- **For the private sector:**
  - Join the Partnering for Cyber Resilience initiative; commit to the Principles
  - Develop a pervasive culture of cyber awareness and resilience
  - Commit to responsibility and accountability for developing the organization's level of cyber resilience
  - Promote the spread of best practices throughout supply chain
  - Engage in policy debate, and where possible, align under common core principles and commitments as a first step towards harmonizing policy needs
- **For the public sector:**
  - Work towards a flexible, but harmonized criminal justice capabilities framework
  - Engage private sector and adjacent policy domain experts to identify potential unintended consequences of policy development in advance
  - Ensure individual protections and foreign jurisdiction counterparts to share lessons learned and improve harmonization
  - For public agencies: join the Partnering for Cyber Resilience initiative; commit to the Principles (of Cyber Resilience)
- **For the private and public sectors together:**
  - Commit to develop robust and sustainable public-private partnerships for a resilient cyber environment, based on clear and

    - mutually agreed assignment of roles and responsibilities and the principle of accountability
    - Explore the need for the development of a cyber-risk market
- **For academia:**
    - Promote the concept of economics of cybersecurity to non-specialist fields
    - Advance research on information sharing and the link between cyber resilience and national competitiveness[12]

WEF and other public organizations and NGOs promote the development of guidelines for policy and criminal justice communities. They promote their implementation as part of a total security and safety regime for the cyber environment.

THE FUTURE ISSUE

We submit that, first and foremost, there is one salient issue for the implementation of smart security in the smart city. Moreover, that issue is political accountability. All the stresses associated with the implementation of information security in a business are present in the political life of the city. However, the metrics of success, and the accountability for failure, is much more diffuse. If the traffic system fails and the city is paralyzed, who will be called to account? Elected leaders are in for their terms, so there will not be any immediate sanction (absent an impending election). Bureaucrats who may be responsible will only be held to account if it serves a political purpose, from political leaders who may or may not understand enough about these issues even to know whom to hold accountable. Even political leaders concerned about the future must balance expenditure for potential risk management against current demands. This all seems to shift the political will to act off to future political leaders and future generations.

This future issue is, in fact, a massively complex one, particularly given the unique American system of federalism and the practices in some states for the development of responsibility to local entities. In one recent infrastructure failure, a U.S. city switched municipal water supply only to find it was now poisoning its citizens with metallic lead in the water; yet, no political leader has been held to account beyond offering apologies (with some bureaucrats resigning their positions).[13] Jurisdictional control of factors within the city may lie with multiple political entities at various levels, including federal, state, local, and local special-purpose entities. Some of these have been intentionally designed to insulate them from popular political will, such as public utilities given appointed boards and even limited taxing power. All may be shielded, to a greater or lesser degree, by sovereign immunity from liability for even significant wrongdoing. Therefore, when traffic systems fail under a cyberattack and people die, there may only be that diffuse, downstream political accountability to demand change.

Without the political will to protect the people of the smart city, there is not going to be any safety.

CONCLUSION

The smart city absolutely demands smarter security, even as we struggle to define what that means. The lack of a coherent approach toward the identification and remediation of attacks on nodes of security will only mean growth in open targets. The leadership of private organizations and NGOs, the academy, and core governmental agencies, is vital to build the foundations for protection. This must be embraced by all the entities and organs of the city. This requires a strong political effort to implement and maintain a safe and secure smart city—every smart city—before things go very, very wrong, and people—men, women, and children—are hurt by the evil of others who exploit the wonders the city can offer.

ENDNOTES - CHAPTER 5

1. The author thanks Joseph D. Losavio for his assistance in research, writing, and developing the original concept paper of this chapter and China Tom Miéville for his insistence that we look at the city in a different way. An earlier version of this chapter appeared as the paper Adel S. Elmaghraby and Michael Losavio, "Smarter Cities Demand Smarter Security," Presented at The City University of New York (CUNY), City College, Cyber Infrastructure Protection (CIP) Conference in New York on October 15, 2015.

2. Adel S. Elmaghraby and Michael M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," *Journal of Advanced Research*, Vol. 5, Iss. 4, July 2014, pp. 491-497, available from *dx.doi.org/10.1016/j.jare.2014.02.006*.

3. Ivan Berger, "IEEE's First Smart City Conference to Meet in Mexico's First Smart City: Guadalajara gathering to cover data collection, analytics, and privacy," the institute: The IEEE news source, August 7, 2015, available from *theinstitute.ieee.org/*.

4. Jung Hoon Lee, Marguerite Gong Hancock, and Mei-Chih Hu, "Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco," *Technological Forecasting and Social Change*, Vol. 89, November 2014, pp. 80-99, available from *dx.doi.org/10.1016/j.techfore.2013.08.033*.

5. Cesar Cerrudo, "Brief: Keeping Smart Cities Smart: Preempting Emerging Cyber Attacks in U.S. Cities," Institute for Critical Infrastructure Technology, June 25, 2015.

6. Elmaghraby and Losavio, "Cyber security challenges in Smart Cities," pp. 491-497.

7. Cesar Cerrudo, "An Emerging US (and World) Threat: Cities Wide Open To Cyber Attacks," *White Paper*, Securing Smart Cities, May 2015, p. 8, available from *securingsmartcities.org/wp-content/uploads/2015/05/CitiesWideOpenToCyberAttacks.pdf*, accessed September 8, 2015.

8. Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," 8th USENIX Workshop on Offensive Technologies (WOOT '14), San Diego, CA, 2014, available from *https://www.usenix.org/conference/woot14/workshop-program/presentation/ghena*, accessed September 13, 2015; Cesar Cerrudo, "Hacking US (and UK, Australia, France, etc.) Traffic Control Systems," April 30, 2014, IOActive blog, available from *blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html*, accessed September 13, 2015.

9. Eric Basu, "Hacking Insulin Pumps And Other Medical Devices From Black Hat," *Forbes*, August 3, 2013.

10. Craig Timberg, "Hacks on the highway: Automakers rush to add wireless features, leaving our cars open to hackers," *The Washington Post*, July 22, 2015.

11. World Economic Forum (WEF) and Deloitte, "Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience," Geneva, World Economic Forum, May 31, 2012, p. 7, available from *https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience/*.

12. *Ibid*., p. 7.

13. Claire Groden, "How Michigan's Bureaucrats Created The Flint Water Crisis," *Fortune*, January 20, 2016, available from *fortune.com/flint-water-crisis/*, accessed January 27, 2016.

CHAPTER 6

ANTICIPATING THE NATURE AND LIKELIHOOD OF A CYBERTERROR COMMUNITY

Max Kilger

INTRODUCTION[1]

The evolutionary path of digital technology over the past 30 years has brought with it many changes in the technical world, including business information technology (IT), government infrastructure, and military logistics and weaponry. It also has had a profound effect on our social world, including how we communicate, exchange information, participate in the consumer marketplace, how we earn a living, and much more.

When we look more closely, however, we see even more profound and unexpected effects of digital technology in our social world. In particular, one of the more interesting consequences of this technological progression is the formation of unique social communities centered on these emerging technologies. This chapter examines the mechanisms surrounding the appearance of specialized communities, technology-centered communities specifically, and also investigates some of the unique characteristics that make these subpopulations of special interest to social scientists, as well as policymakers and information security professionals.

My thesis suggests that there have been two major waves or epochs during this digital revolution that are marked by the emergence of a specialized technical community. The first specialized community that is hypothesized to have emerged is the hacking community, which can trace its roots to some of the early technical pathfinders and early adopters of digital technology. The second specialized community is the more recent development of a cybercrime community, where the lure of significant financial and resource gain has banded many individuals together to form a very active and quickly evolving community dedicated to the acquisition of financial and other valuable assets through illegal or quasi-legal means. Finally, it is hypothesized that there is a third specialized technical community gestating in the digital world—the emergence of a cyberterrorist community that embraces members who are using digital technology to achieve their goals, which may include political, social, religious, economic, or cultural objectives.

In this chapter, we will first examine some of the theoretical elements and processes involved in the emergence of technically oriented communities. It is suggested these collections of people are instances of social movements that have embedded themselves in technologically oriented communities. We then take a detailed look at the two currently existing communities—the hacking and the cybercrime communities—to examine their nature and how they may have emerged. Finally, we turn to investigate the hypothesized emergence of a third community, a cyberterrorist community, and suggest what the characteristics of such a community might look like, as well as how likely it is that this social movement and community will emerge.

TECHNOLOGY-FOCUSED COMMUNITIES AS SOCIAL MOVEMENTS

One of the first questions to be asked is if these technology-focused communities (e.g., the hacking and cybercrime communities) are actually social movements. Charles Tilly defines a social movement as follows:

> It consists of a sustained challenge to power holders in the name of a population living under the jurisdiction of those power holders by means of repeated public displays of that population's worthiness, unity, numbers, and commitment.[2]

Each of these communities, it could be argued, likely appears to be a population mounting a sustained challenge to power holders, and simple examples can provide support for this idea. In the case of the hacking community, one of the main challenges to power holders they pose is the idea that information should be free and that freedom of information will transform society as we know it.

Matthew McCarthy describes the one-sided control of information as an instance of the asymmetry of information, and he performs a traditional social movement framing analysis of two groups, Anonymous and WikiLeaks, which are attempting to wrest control of information from power holders and restore information symmetry by distributing this information to all.[3] These groups argue that all information should be freely available, that the asymmetrical control of information promotes unequitable control of resources and power, and that their actions are worthy of support by society in general.

The phrase "We are legion" is a phrase that is often uttered by a number of members in various groups within the hacking community, in particular by hacktivists, when responding to public statements concerning their actions or the nature of their hacktivist group. This statement finds its roots in a statement found in the New Testament of the Christian Bible, and it is said to have been uttered by Jesus Christ when asked his name and he replied, "My name is Legion, for we are many."[4] This suggests that the hacking community's desire is to communicate the fact that there are a large number of members that comprise their community, in line with Tilly's definition of social movement.

The characteristics of unity and commitment can be found within the hacking community in a number of examples. Organizations such as the Free Software Foundation, and the public portions of the software development website GitHub, provide developers with development tools, software depositories, and collaboration space for the development and distribution of millions of lines of code belonging to free and open source software without charge.[5] Hacking conferences such as DEF CON in Las Vegas, CanSecWest in Vancover, BruCon in Brussels, and Hack in the Box in Malaysia provide meeting places where hacker collaborators that have been working long distance can meet up with their colleagues and other members of the hacking community to share code, stories, food, alcohol, and otherwise strengthen their social bonds and ties.

In the case of the cybercrime community, the argument is a bit more complex. While both the hacking community and the cybercrime community contain members who commit illegal acts in the digital world, members of the cybercrime community are almost entirely, by definition, involved solely in the pursuit and perpetration of acts of illegal online behavior, which are often virtual counterparts of traditional crimes such as theft, counterfeiting, burglary, and extortion. Members of the hacking community, on the other hand, often commit some of the same illegal acts that cybercrime community members do, such as unauthorized access to computer systems, but generally refrain from committing most of the financially motivated digital analogues of real-world crimes.

It can be argued, however, that the cybercrime community may be held out as an example of a social movement as defined by Tilly. The power holders in the case of the cybercrime community turn out often to be multi-national corporations who hold and wield disproportionate amounts of financial assets or intellectual property. Even though many cybercriminals focus on financial crimes such as stealing and using financial instruments such as credit cards, financial credentials, and other financial instruments that often belong to an individual, the true victim in the end turns out to be the large multi-national financial institutions who must make up the losses to individual consumers and clients as well as bear the burden of the costs of the crime. Thus, it could be claimed that their cause is worthy because they are redistributing wealth that is being held by large national corporations; or alternatively, some may use the not necessarily true but often expressed idea that the crime is being committed against multi-national organizations, and therefore there are no real victims, as a means of providing a purpose worthy of support from the larger population.

In terms of Tilly's social movement characteristics regarding the number of individuals who would classify themselves as members of the cybercrime community, it is difficult to determine how many there actually are, given the pressure from both national and international law enforcement organizations to shut down their enterprises and arrest their members. However, it could be possible to substitute the considerable financial losses attributed to cybercrime as one proxy measure of the size, and more importantly the impact, of the cybercrime community. For example, the Center for International Studies estimates that the total global loss due to cybercrime in 2014 was approximately $400 billion.[6]

As for Tilly's concepts of unity and commitment, there are several examples that may help substantiate the case for the existence of a cybercrime community. Thomas Holt describes in detail the dynamics of cybercrime marketplaces.[7] These marketplaces often show organizational sophistication where cybercriminals band together to offer guarantor services for the exchange of money for products and services such as stolen credit cards, financial credentials, malware, spam and phishing services, and Denial of Service (DoS) attack services, among others. There are also reputational mechanisms put in place by the cybercriminal community so that customers have confidence they will receive the products and services they have purchased. These reputational services also assist in providing vetting obstacles so members of the cybercrime community are less likely to admit an undercover law enforcement officer to their forum. There appears to be an uncommon unity among online thieves and criminals that is often lacking in more traditional crime scenarios, with the possible exception of organized crime entities.

Given that the evidence and discussion above may lead one to provisionally accept the idea that the hacking and cybercrime communities are each a special instance of an online social movement, then the question is how to approach the analysis of these social movements in relation to the potential formation of a cyberterror community. Theories of social movements can broadly be categorized into one of four frameworks: political analysis, frame analysis, resource mobilization theory, and new social movement theory.[8] For the purposes of this discussion, a variant of the new social movement theory will be applied to the examination of the hacking community, the cybercrime community, and the conjectured emergence of a cyberterror community.

New social movement theory emerged in the 1960s and focuses upon issues of identity, equality, direct participation, and democracy as outlined by Noriko Hara and Bi-Yun Huang.[9] This theory provides unique utility in explaining the role of information and communication technology (ICT) in social movements, a particularly useful characteristic given the technological nature of the communities and social movements under study. The next section lays out one particular variation of new social movement theory, as developed by Hara and Huang, that we will apply to our analysis of the hacking and cybercrime communities as well as to the likelihood and nature of the emergence of a cyberterror community.

INFORMATION AND COMMUNICATION TECHNOLOGIES AND SOCIAL MOVEMENTS

The adoption of ICTs by social movements has had a profound effect on many dimensions and characteristics of social movements, including modes of communication, the formation and maintenance of collective identity, and methods of mobilization. Hara and Huang provide a comprehensive look at online social movements and define their use of ICTs in five different dimensions. The first dimension is the use of ICTs as a source of resources. These resources might include financial resources, the ability to communicate and disseminate information, and the ability to coordinate the involvement of members of the movement. ICTs can often facilitate a rather effective fundraising effort on a much broader and indeed global scale compared to traditional fund raising channels.

Secondly, Hara and Huang identify ICTs as operating as a framing function as defined in traditional social movement theory. Social movements can frame and define the collective understanding that their movement represents. It can also help individuals involved in the movement frame and associate their individual experiences within this larger collective understanding. This framing process can in turn facilitate the mobilization of collective action. For example, Noriko Hara and Zilia Estrada have examined how communication channels such as websites and email have the ability to mobilize both members of the social movement as well as those individuals that may not formally identify with the movement.[10]

The third dimension proposed by Hara and Huang is the use of ICTs in supporting collective identity. Collective identity is a key component of social movements that has received considerable theoretical attention by social movement theorists. Identification with a social movement provides its members with a sense of collective identity that can be shared with other members of the movement. It also serves as a catalyst for mobilization that allows members of the movement to identify other members so that they may coordinate actions and share the execution of tasks that contribute to the central cause of the social movement. The use of symbols that represent the social movement on websites and in online videos can contribute to this sense of collective identity.

Hara and Huang identify the fourth dimension as the role that ICTs play in the mobilization of members of the social movement. A social movement may utilize email, Twitter, and short message service (SMS) texts that contain messages and identity symbols of the social movement that can be utilized to reinforce the legitimacy and "rightness" of mobilization directions and actions in real time to individuals who are participating in actions being coordinated under the auspices of the social movement. Members of a social movement may also utilize websites and other ICT channels to persuade others who are not members of the movement that the objectives of the movement are worthwhile. ICTs also play an important role in mobilizing members of its social movement and community into direct action. The speed and ubiquity of digital communications means that members can be mobilized very quickly, and those mobilization efforts can be deployed from anywhere there is a connection to a widespread digital network like the Internet.

The fifth and final dimension that characterizes ICTs in their role in social movements, as proposed by Hara and Huang, is that of providing a virtual space within which the social movement can conduct its activities. Unlike traditional, historical social movement actions, many of the actions that ICT involved social movements conduct can occur virtually in the digital world. That is, while ICTs are often utilized in coordinating efforts to mobilize members for movement organized activities in a particular geolocation such as happened in the Arab Spring, ICTs often provide a digital space that can be used by movement members to virtually assemble as well as serve as a launching platform from which digital actions promoting the cause of the movement can be launched.[11] Similarly, this virtual, digital space can serve as the environment from which to initiate actions against persons and organizations that stand opposed to the causes and objectives of the social movement. These actions might include email campaigns, social media posts on Facebook, Twitter feeds, and blog posts that carry the messages of the social movement.

All of the previous discussion up to this point has framed ICTs mainly as a communications channel for distributing the cause, objectives, and messages of the social movement, whether for the purposes of generating solidarity among the members of the movement, mobilizing members for a particular action, targeting specific non-member individuals or organizations with specific messages, or exposing the general public to the movement's core goals along with appeals to action, whether to contribute funds to the movement, or join them in their cause.

However, the hacking and cybercriminal communities as social movements under investigation are different in terms of the relationship of technology to the movement. That is, while the nature of the relationship between ICT and social movement dimensions outlined by Hara and Huang are undoubtedly at work in both of these communities, technology plays a much more central role in these movements than might be found in other more typical social movements under study. Technology is in fact embedded in the core framework of these communities and the social movements they represent.

In the case of the hacking community, their very reason for existence can be traced to the development of new digital technologies. Without the innovations that have heralded the evolution of the digital revolution, the emergence of a hacking community might have been in very grave doubt. Similarly, without the digital tools to create and deploy malware along digital networks, the emergence of a cybercrime community and social movement would not have taken place. Therefore, in our examination of the emergence, transformation, and maturing of both the hacking and cybercrime communities, we may need to extend and stretch the analytical platform provided by Hara and Huang in order to provide a more comprehensive picture of their respective social movements. In addition, a few liberties may need to be taken with this theoretical platform when examining the likelihood and nature of the emergence of a cyberterror community and its associated social movement.

The following sections examine the two technology-focused communities, and accompanying social movements formally labeled as the hacking community and the cybercrime community, through the theoretical lens of Hara and Huang. In addition, it is hypothesized that the cybercrime community is a social movement spin-off of the temporally prior hacking community and its associated social movement. After examining the nature of the cybercrime community, attention will be turned to the idea that a cyberterror social movement will arise as a spin-off movement of the cybercrime movement, and a cyberterror community will form. This examination will explore the intertwining of ICTs and the potential emergence of a cyberterror collective, as well as speculate on the likelihood of this event occurring.

Epoch 1: Information Communication Technologies and the Hacking Community.

The origins of the computer hacking community can be traced back to at least the early 1960s; one of the most unique things about the community and social movement is that the community itself was, and still is, the primary source for the emergence of new ICTs. That is, rather than having to depend upon existing technologies for internal communication among its members, external communications toward non-members, and society in general, the hacking community has the skills, expertise, and cultural motivation to develop new ICTs to fulfill whatever need arises. When it was necessary to communicate securely amongst themselves, the community developed secure encryption technologies such as Pretty Good Privacy (PGP), which in turn spawned secure communications such as hushmail and many other encrypted forms of communication and data storage.[12] Similarly, when the need emerged to be able to solicit funds, as well as securely and covertly move financial assets from place to place or group to group, they developed anonymous currencies such as Bitcoin to accomplish this task.[13] Also significant was the development of data and code transport systems early on to be able to share with other members of the community as well as collaborate on large collections of computer code, the primary raison d'être for the social movement itself.

ICTs also play a crucial role in frame alignment processes of the hacking community. David Snow and his colleagues describe one type of frame alignment in the form of frame bridging, which is:

> At this level of analysis, frame bridging involves the linkage of an SMO [social movement organization] with what McCarthy (1986) has referred to as unmobilized sentiment pools or public opinion preference clusters. These sentiment pools refer to aggregates of individuals who share common grievances and attributional orientations, but who lack the organizational base for expressing their discontents and for acting in pursuit of their interests.[14]

In this case, ICTs play the important role of reaching out to individuals who do not consider themselves part of the hacking community but share their goals and values and, in particular, some portion of their skills and expertise. The possession of skills and expertise is an important linkage in the frame alignment process because of the fact that the hacker community is a strong meritocracy, and in order for individuals or groups to join the community, they must possess and indeed demonstrate skills and expertise in one or more technical areas such as coding, operating systems, network protocols, information security, or other relevant topics.[15]

Collective identity has been an important issue for some time within the hacking community. This community has been negatively defined for many years by members outside of the community, and they have often been labeled as deviants or criminals. Self-identification with a social movement that has been largely labeled in such negative terms by the larger society poses some significant challenges, not only in the ability to attract new members into the community, but also by impairing the ability of already existing members to attract resources and even appear in public places.

There has been considerable interpersonal, intergroup, and intra-community conflict over the use of the term hacker as a self-identifying label. A significant portion of this conflict is due to the nature of the hacking community as a strong meritocracy, and due to the lack of bandwidth of various ICT technologies to convey verbal and nonverbal cues that would allow members of the community to resolve these status based skirmishes. It has been suggested that the various methods by which members of the hacking community communicate, such as email, Internet Relay Chat (IRC), blogs, and even video chats, completely either block or substantially degrade the verbal and nonverbal cues that are often necessary for individuals to resolve status conflicts.[16]

When individuals identify themselves with the hacking community and social movement, this is in fact a formal claim of competence and expertise in one of the previously mentioned technical areas of digital computing or networking. If this occurs over ICT communication channels, it is difficult for the self-identifying individual or group to provide traceable or believable evidence of their competence. Related to this idea is the conjecture that hacker conventions serve a vital function in that they allow individuals from the hacker community to interact face-to-face where there is ample opportunity for verbal and nonverbal cues to be exhibited and interpreted by individuals, which in turn helps resolve the status ambiguity and reduces the conflict experienced within the hacker community and social movement.[17]

Additionally, the ability of ICTs to mobilize the members of a social movement or community is a critical capability for the hacking community. This is particularly true because the members of this community are often geographically distant from each other; therefore, traditional forms of mobilization for social movements that involve marches, protests, and other forms of mobilization are often not logistically feasible for these members. ICTs for the most part function as a mobilization channel for the social movement in terms of rallying its members to virtual or online actions, particularly where more traditional methods involve propinquity.

This rallying process may take the form of posting statements on blogs and forums that support the particular action that the community has adopted for the cause. It might also appear as a virtual or digital attack on another organization. This virtual attack might take the form of a website defacement or something more serious such as the compromise of data servers for the organization, and the exfiltration and publication of damaging or embarrassing information. It might also take another more positive path, such as writing software that allows individuals in countries with repressive regimes the ability to surf the web without fear of being identified and punished.[18]

ICTs provided the hacking community and social movement with its own virtual space within which to exist. It is important to note here again that for the hacking movement, ICTs are not just communication channels, funding sources, and mobilization pathways, but they are the very environment that allow the hacking community and its members to exist. Without this digital environment, the hacking movement and its associated community would likely not have emerged and proceeded to persist over the past few decades. It is the home environment for these entities, and without it, these communities might not exist.

Finally, there comes the concept of social movement spin-offs. The hacker community and its associated social movement have been in existence for 5 decades, and it is still a very strong community with a large number of members. However, over the years, this social movement has changed in many ways, and in some respect, it is very different from its humble beginnings in largely academic and university circles. Some of this change is posited to have occurred due to the influx of money and commercialization of the community's virtual environment, in particular the Internet. The social structure for the hacking community for two distinct times, 1994 and 2003, has been mapped out; it has been hypothesized that the decline in the incidence of key social structure dimensions within the community, such as status, magic/religion, and aesthetic, were due to the influx of money and commercialization of the products and services that members of the hacking community were developing. These products and services were being developed in the members' commercial day jobs. That is, often projects that they were working on independently as members of the community suddenly had become imbued with commercial value.[19]

As these monetarily driven changes in the social structure of the hacking community advanced, this in turn encouraged the emergence of a spin-off social movement from the hacking social movement. This spin-off is the cybercrime community and associated social movement, that has at its core the principle of utilizing ICTs for the direct illegal acquisition of money, as well as credentials that lead to other financial resources, the illegal acquisition of data, the acquisition of health records, and other intellectual property that can be converted into money through sale or extortion. It also led to the rise of services, such as Distributed Denial of Service (DDoS) attacks, that can be utilized to damage a competitor or force an organization to pay to have the attack cease. Similarly, this has led to the development of ransomware attacks by cybercriminals, where valuable data and servers are encrypted and a payment to these criminals must be made in order to have the data decrypted. These are by no means all of the schemas by which members of the cybercrime community acquire financial assets, but they are common examples.

Nancy Whittier, in her exposition on the consequences of social movements on each other, describes how social movements may spin-off from each other, and that this process may not only give rise to movements with similar structures and objectives, but also to opposing movements.[20] The spinoff of the cybercrime movement from the hacker movement is particularly notable because, since the early years of the hacking movement, there was strong opposition by community members to derive money or other financial gain through illegal means that were facilitated through efforts, on their part, utilizing their skills and expertise in ICTs. Individuals in the hacking community who hacked for profit in these early days were ostracized and shunned to the point where they were forced to seek out others who had similar objectives and motivations. The injection of a multi-dimensional element such as money into any social system often changes it in powerful and sometimes irreparable ways.[21] In the next section, Epoch 2, we examine the ICT evolution where the rise of the cybercrime community and its associated social movement is still steadfastly underway.

Epoch 2: Information and Communication Technologies (ICTs) and the Cybercrime Community.

ICTs are deeply and permanently integrated into the emerging social movement that embraces the foundations of cybercrime. These technologies provide members of the cybercrime movement with the ability to accumulate large numbers of financial credentials and value-laden data as well as intellectual property. Just as in the early days of the banking industry where banks and other financial institutions were focal points for the aggregation and accumulation of money, precious metals, and other valuables that were attractive targets for traditional criminals, ICTs have accumulated these same kinds of assets as well as some new types (e.g., Bitcoin) on a scale that is magnitudes larger than ever before imagined.

Information and communication technologies have also facilitated two important components that have served to encourage the rise of the cybercrime community. The first is to enable members of this community to envision a path to access the financial assets that do not depend upon geographical propinquity but rather on the skills and expertise of the members themselves by traversing complex digital networks that exchange data with each other. In particular, the advent of the Internet and the inclination of commercial and governmental organizations to link their digital networks to it have provided members of this social movement with an almost unlimited opportunity to obtain these assets illegally.

Finally, ICTs have spawned a significant war chest of software development tools with which members can develop code and tactics that are designed to gain them unauthorized worldwide access to servers holding financial, health, governmental, and intellectual property assets. This access can be gained is through a direct attack on the servers themselves, an indirect attack through attached networks and servers, or through other means such as phishing authentication credentials from unsuspecting individuals.

In terms of Hara and Huang's second criteria of the framing function, the primary attractant in encouraging members to join the community is the prospect of acquiring significant amounts of money in short periods of time with a disproportionately small amount of effort and investment required. Here, the frame alignment problem is more one of often convincing individuals who might otherwise be law-abiding citizens to realign their internal value system so that their values align with the larger principles of the cybercrime social movement and community. In some cases, such as the class of individuals known as money mules, it may not be completely clear to the individuals that they are participating in a criminal enterprise, so there is little frame alignment that needs to be accomplished.[22] In other scenarios, traditional criminals whose value system already significantly aligns with the value system of the cybercrime community may need very little adjustment to accomplish a shift in frame alignment between their current system of values and that of the cybercrime community. Further, it may be the case that some individuals in the hacking community that currently hold the idea of making money illicitly through development of malicious code repugnant will abandon their membership in the hacking community and will instead follow the frame alignment path to integrate themselves and their actions into the cybercrime community.

The third dimension of Hara and Huang's theoretical strategy is detailing how ICTs support collective identity. Now, this is an interesting situation in the case of the cybercrime social movement. Because the primary objective of the community is the commission of illegal acts for the purpose of unlawfully gaining access to financial and other valuable assets, there is some inhibition for publicly identifying with the cybercrime community. While the hacking community used to face this in the early days of the movement when hackers were universally disparaged as deviant actors committing unethical and often illegal acts, in recent years members of the hacking social movement have gained considerably in their quest for acquiring a more positive image. This quest has been enhanced by the role that Hollywood has played in reforming the image of members of the hacking community in movies and television (TV) programs. Thus, the role of deviant or criminal has been passed on from the hacking community to the cybercrime community.

There is another facet to the collective identity at work in the cybercrime community, which is the familiar one of brand image and promotion. Internally among the members of this social movement, there is the necessity for actors to portray their products and services that are used to gain unauthorized access to financial or other valuable assets in a positive light, which is very similar to the challenges that legitimate businesses must face in promoting a positive image of their product or service in order to maintain and increase sales of those items.[23] In addition, cybercrime community members often belong to a specific forum or marketplace where there are socialized norms and rules in place that protect both buyers and sellers of stolen financial credentials.[24] Belonging to one of these regulated underground cybercrime marketplaces provides members of the cybercrime community with a collective identity via the marketplace, such that they may share in the reputation of that marketplace as being a place where exchanges of funds for products and services are fair and honest.

The collective benefits of Hara and Huang's fourth dimension concerning ICTs and their ability to mobilize members of a social movement can be found in the cybercrime community when it comes to norm regulation and social control within the community itself, and in particular for specific underground marketplaces. Criminal marketplaces are somewhat unique in that they have to be self-policing—there is no option for members of the community to reach out to traditional policing forces to help resolve disputes and report issues such as fraud on the part of other community members or customers. Therefore, as Holt has discussed, there are normative orders within the cybercrime marketplaces that heavily rely upon communication via ICTs to facilitate things like the transfer of payments through guarantors for products and services. In addition, ICTs play an especially critical role of social control in the cybercrime marketplaces, as individual buyers and sellers often need to acquire reputations as reliably transacting honest exchanges. Individuals who attempt to cheat others in the cybercrime marketplace are known as rippers, and ICTs are used in the key role of mobilizing the rest of the community against these norm violators.

Finally, the fifth dimension in Hara and Huang's schema involves the use of ICTs as a virtual space for the social movement. This is probably one of the most important functions of ICTs for the cybercrime community. The community needs a location to establish its marketplace, and rather than a historical real-world location such as a souk or town square, the cybercrime community uses cyberspace as its covert marketplace.

Note that not just any spot in cyberspace will do for a cybercrime marketplace. Typically, these marketplaces emerge in what is known as the dark web, servers that have their Internet Protocol (IP) addresses hidden and are usually reached through various and more secure encrypted networks—very typically, Tor networks. The issue of course is that these cybercrime marketplaces must make some attempt to hide from law enforcement as well as the general public—whose pursuit and public outcry might add additional pressure to these marketplaces. Therefore, finding one's way to these cybercrime bazaars is a bit more difficult than just traditionally surfing the web. At the same time, cybercrime community members cannot hide their storefronts so effectively that their customers cannot find them. Often the initial search for a cybercrime storefront involves using ICTs to find various lists on Reddit or a number of specialized Wiki servers that provide lists of websites run by members of the cybercrime community. Without a somewhat protected virtual space that provides cybercrime members with a partially cloaked marketplace where anonymous transactions and payments can be processed via ICTs, it is likely that the cybercrime social movement would not exist in its current large, robust multi-dimensional form.

In summary, as was stated earlier, it is hypothesized that the cybercrime movement and the emergence of a cybercrime community is the result of a number of individuals who were originally members of the hacking community, but whose motivations for malicious online acts evolved into acquiring money and other valuable financial or information-based assets by illicit means.[25] However, once the initial core of the cybercrime movement was established, it is likely that additional members that joined the community may have been either marginal members or more likely non-members of the hacking community. That is, newer members to the cybercrime social movement may have joined without having any significant time in the hacking community proper.

One of the outstanding questions concerning the cybercrime social movement and the cybercrime community is whether or not this community and social movement is here for the long term and is likely to grow. Other ICT-based social movements and communities that have emerged from the hacking community, such as the cyberpunk and cypherpunk communities have risen from the hacker social movement proper, but have not flourished or experienced the exponential growth in the manner that the cybercrime community has. It is likely that the lure of money, as well as the ambiguous prospects of being apprehended, contribute significantly to this noteworthy growth.

Several authors have ventured opinions about the resilience of the cybercrime community. Sadia Afroz and colleagues suggest that if the marketplaces observe the practices that: "1) have easy/cheap community monitoring, 2) show moderate increase in new members, 3) do not witness reduced connectivity as the network size increases, 4) [limit] privileged access, and 5) enforce bans or fines on offending members," that these cybercrime marketplaces and the cybercrime community in general will be sustainable.[26]

Similarly, Martin Libicki and his colleagues suggest that there will be more targets for the cybercrime community as more data becomes digital and connectivity continues to expand.[27] They further suggest a turn away from financial and credit card cyber-theft as the market becomes flooded and their value decreases, while some experts suggest that intellectual property and data breaches will become more popular as currencies in the marketplace. They suggest that some cybercrime actors will migrate from pure cybercrime (black areas) to more gray areas where the legality of the acquisition and exchange of commodities is more in question rather than strictly illegal. They also suggest that "hacking has become little league: everyone starts out early, and spends a lot of time doing it."[28]

Overall, it is likely that the cybercrime social movement and community are here for the long term, as was the hacking community in the previous epoch. It should be noted, however, that it is expected that this community will change significantly over time and that it will likely encourage further theoretical and empirical investigation by social scientists and information security professionals to build a more comprehensive understanding of this community and where its future may lie.

Epoch 3: Information Communication Technologies and the Cyberterror Community.

The final section in this chapter revolves around the idea that the major third epoch to emerge as a result of the synergy between ICTs and social forces in play involves the appearance of a social movement centered around cyberterrorism as well as the emergence of a cyberterror community. The previous discussions regarding the emergence of the hacking movement (see Epoch 1) and the cybercrime movement (see Epoch 2) were useful not only to examine the historical context from which this social movement might arise but it also provides the opportunity to apply some theoretical structure to these communities to better understand them.

In addition, the application of Hara and Huang's theoretical notions about the interplay between ICTs and social movements to these communities in a way builds a theoretical "plank" from which to walk out over the abyss that represents the paucity of research and discussion about the possibilities of the emergence of a cyberterror community in the literature. We will use Hara and Huang's theoretical structural "skeleton" and rely on it for support to fill in the skeleton with conjectures about the nature of an emerging cyberterror social movement and its associated community. We will also use Dorothy Denning's definition to minimize confusion for the reader about what constitutes cyberterrorism.[29] Her definition of cyberterrorism is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Hara and Huang's first dimension looks at ICTs as a resource for the social movement. As one might expect, ICTs provide a fertile ground for communications among cyberterrorists, and social network analysis can be applied by researchers and information security professionals to provide information about the members and nature of the cyberterrorist network.[30] ICTs also provide cyberterrorists with coding and programming resources to develop malware, exploits, rootkits, and other pieces of code that will be deployed in a cyberattack on a prospective target. ICTs also provide the access necessary for cyberterrorists to reach their targets. Unlike traditional terrorism, where physical proximity is generally necessary to successfully deploy an attack, cyberterror attacks can originate from anywhere on the globe against a target anywhere else in the world. Although the Internet is typically utilized as a channel for a cyberattack, this does not necessarily have to be the case; as can be witnessed by the success of the Stuxnet attack, which would qualify by Denning's definition as a terrorist attack on a segment of Iran's infrastructure. This attack was reportedly accomplished when a thumb drive was inserted into a computer somewhere inside the Iranian uranium centrifuge facility.

In terms of Hara and Huang's ICT framing dimension, for a number of years ICTs have functioned as frame alignment mechanisms for the traditional terrorist community when used to radicalize and recruit non-members into their social movement.[31] Although, some researchers suggest that the lack of verbal and nonverbal cues in computer mediated communications lowers the level of trust, and thus makes recruitment of terrorists via the Internet more difficult.[32] However, it would seem likely that recruitment into a cyberterrorist social movement would be less difficult than it would be for recruitment into a traditional terrorist organization. Individuals with the specific coding, information security, operating systems, and digital networking skills necessary to develop code that would be used in a cyberattack are already comfortable communicating and developing trust relationships through ICTs.

In addition, non-members are also likely to have an online presence that will make discovery and contact by cyberterrorist members easier by utilizing websites that promote and nurture radicalization. This method is another way that both cyberterrorists as well as traditional terrorists execute frame alignment processes in the pathway toward recruitment of a non-member into a terrorist or cyberterrorist movement.

The frame alignment process for moving non-members along the path to membership in a cyberterrorist social movement and community may also be influenced by environmental factors. It has been argued that ICTs may have fundamentally changed the power relationship between nation-states and individuals. That is, utilizing ICTs, for the first time in history, may allow an individual to effectively attack a nation-state. The environmental factors influenced by ICTs that may lead individuals to become "civilian cyber warriors" include: the relatively low risk of apprehension; the high probability of success of the attack; the large magnitude of damage that may be inflicted against targets, such as critical infrastructure, and the low investment in hardware, software, or effort necessary to execute the attack.[33]

Hara and Huang's third dimension revolves around the use of ICTs to support and enhance collective identities for social movements. As we have seen in the hacker community, collective identity is an important element of a hacking group's make up. Often there is some symbol, such as the man with the top hat for the LULZSEC group or the Guy Fawkes mask for the Anonymous hacktivist group. Traditional terrorist groups often have logos or icons that identify the group and individual members of the group, and when they feel safe, members of traditional terrorist groups will often identify with their extremist group using these symbols.

Collective identity can also be a powerful motivator for individuals who are susceptible to recruitment when their primary motivation is to feel like they belong to a group or cause of importance. Given the propensity for groups in the hacker social movement to encourage collective identity through a shared community symbol, it is likely that an emerging cyberterror social movement and the members of that community will develop iconic images so that members will have strong feelings of identification with the cyberterror movement. These iconic symbols may make effective markers for identifying an emerging cyberterrorist community for law enforcement and intelligence agencies.

ICTs will also be very useful in mobilizing members of the social movement, as described by Hara and Huang. This may be particularly true when the situation calls for synchronizing multiple cyberattack efforts among distinct team members of the cyberterror movement. It may also be the case that mobilization of the cyberterror community might take place in response to a concerted effort or specific nation-state campaign against a specific ethnic group, country, or even against the cyberterror community as a whole. As the cyberterror movement grows, mobilization of this community against external cyberattack may become a more large scale event, and there is the possibility that the cyberterror movement might develop advance plans to be activated in the event of attack by one or more nation-states or security services.

It should also be noted that the scope of motivations for members of the cyberterror social movement might potentially be much more varied than the traditional geopolitical motivations assigned to terrorist groups. It may be the case that a cyberterror act could be defined as an instance of a malicious online act; so any of the six traditional motivations for a malicious online attack normally applied to members of the hacking community may also apply to members of the cyberterror community.[34] This could considerably enlarge the scope of reasons for a cyberattack as well as the size of the pool of individuals who might be motivated to pursue such an attack. As an example, in a recent study by Holt and his colleagues, it was discovered that between one and two percent of the study respondents were willing to inflict a serious cyberattack on either a foreign country or their own homeland in response to actions by that nation-state that harmed their fellow citizens.[35]

The final dimension that Hara and Huang utilize in their schema is that of the nature of ICTs operating as a virtual space or environment for cyberattacks. If you look at this idea from the perspective of a member of the cyberterror community, it can be seen that most or all of the actions that the cyberattacker takes in preparing and executing the cyberattack typically occur within cyberspace. On the other hand, it is likely that some of the consequences of the cyberattack may occur in the real world, including attacks on electrical generators causing explosions, a chemical plant causing leaks, or radiation leakage from a compromised nuclear power plant. This schism or bridge between the two worlds, virtual and physical, may have some important consequences for the cyberterror social movement. Evidence of physical destruction has a much more powerful impact, both on the victims of the terrorist attack as well as the perpetrators, than might be the case of the consequences of a cyberattack. While traditional terrorists anticipate significant physical destruction and loss of life, it is much less clear what effect these real-world consequences might have on cyberterrorists who are operating almost exclusively in a virtual space.[36] Being able to witness the physical effects of a cyberattack may encourage or embolden members of the cyberterror community as well as generate more widespread and serious fear among both the victims of the cyberattack as well as innocent bystanders.

Finally, the last segment of this discussion is where an estimate of the likelihood of the formation of a cyberterror social movement and creation of its associated community is undertaken. Without the benefit of the application of some theoretical structure via Hara and Huang and a comparison of the prior epochs and their communities, this exercise might be considered almost a wild guess. However, having conducted some very preliminary examinations of the two prior communities through a theoretical lens and projected that lens onto a hypothetical third epoch that contains a cyberterror community, a little of the “wild” might be able to be taken out of that descriptive label. Given the reasonable fit of a number of the potential characteristics of a cyberterror movement within the simple theoretical structure of Hara and Huang and some of the similarities of the cyberterror community in relation to the hacker community in Epoch 1, and to a lesser extent to the cybercrime community in Epoch 2, the evidence suggests that there is a significant likelihood that within the next few years we will see the emergence of a fledgling cyberterror movement and its associated community. It is difficult to determine the exact probability of this event occurring, but if one were forced to express that probability in terms of buckets—low, medium, or high probability of occurring—it is most plausible that this probability lies somewhere between the middle of the medium category and the bottom of the high category.

This emergent cyberterror community is likely to inherit some of the "deoxyribonucleic acid (DNA)" of the cybercrime community; that is, some of the characteristics and elements present in the cybercrime community are likely to show up, perhaps in slightly altered form, in the emerging cyberterror community. Additionally, because the cybercrime community in the same manner inherited some of the social structure DNA of the hacking community, the cyberterror community may also be likely to exhibit traces of social elements that are present in the hacking community. If a cyberterror community should emerge, which it seems is likely to happen, it will be interesting to note which of these inherited elements will surface in this spin-off social movement. It remains to be seen what the future holds for the phenomenon of cyberterror.

ENDNOTES - CHAPTER 6

1. An earlier version of this chapter appeared as the paper Max Kilger, "Anticipating The Nature and Likelihood of a Cyberterror Community," Presented at The City University of New York (CUNY), City College, Cyber Infrastructure Protection (CIP) Conference in New York on October 15, 2015.

2. Charles Tilly, "From Interactions to Outcomes in Social Movements," in Marco Giugni, Doug McAdam, and Charles Tilly, eds., *How Social Movements Matter*, Minneapolis, MN: University of Minnesota Press, 1999, pp. 253-270.

3. Matthew T. McCarthy, "Toward a Free Information Movement," *Sociological Forum*, Vol. 30, Iss. 2, June 2015, pp. 439-458.

4. Jesus Christ, *The New Testament*, Mark 5:9.

5. For a more comprehensive discussion of the beginnings and the principles behind the free software movement, see Eric Raymond, "The Cathedral and the Bazaar," *Knowledge, Technology and Policy*, Vol. 12, Iss. 3, September 1999, pp. 23-49.

6. McAfee and the Center for Strategic and International Studies (CSIS), *Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II*, Washington, DC: McAfee and Center for Strategic and International Studies, June 2014.

7. Thomas J. Holt, "Examining the Forces Shaping Cybercrime Markets Online," *Social Science Computer Review*, Vol. 31, Iss. 2, 2013, pp. 165-177.

8. David Hess, Steve Breyman, Nancy Campbell, and Brian Martin, "Science, Technology, and Social Movements," in Edward J. Hackett, Olga Amsterdamska, Michael E. Lynch, and Judy Wajcman, eds., *The Handbook of Science and Technology Studies*, 3rd ed., Cambridge, MA: MIT Press, 2007, pp. 473-498.

9. Noriko Hara and Bi-Yun Huang, "Online Social Movements," *Annual Review of Information Science and Technology*, Vol. 45, Iss. 1, 2011, pp. 489-522.

10. Noriko Hara and Zilia Estrada, "Analyzing the mobilization of grassroots activities via the Internet: a case study," *Journal of Information Science*, Vol. 31, Iss. 6, 2005, pp. 503-514.

11. Philip N. Howard and Muzammil M. Hussain, "The upheavals in Egypt and Tunisia: The Role of Digital Media," *Journal of Democracy*, Vol. 22, No. 3, July 2011, pp. 35-48.

12. For an informal historical review of PGP see Adam Back, "PGP Timeline," cypherspace, n.p., n.d., available from *www.cypherspace.org/adam/timeline*, accessed September 2015.

13. Daniel Folkinshteyn, Mark Lennon, and Tim Reilly, "A Tale of Twin Tech: Bitcoin and the WWW," *Journal of Strategic and International Studies*, Vol. 10, No. 2, 2015.

14. David A. Snow, E. Burke Rochford, Jr., Steven K. Worden, and Robert D. Benford, "Frame Alignment Processes, Micromobilization, and Movement Participation," *American Sociological Review*, Vol. 51, No. 4, August 1986, pp. 467.

15. Max Kilger, "Social Dynamics and the Future of Technology-Driven Crime," in Thomas J. Holt and Bernadette H. Schell, eds., *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications,* Hershey, PA: IGI-Global, 2010, pp. 205-227.

16. Cecilia L. Ridgeway, Joseph Berger, and LeRoy Smith, "Nonverbal Cues and Status: An Expectation States Approach," *American Journal of Sociology*, Vol. 90, No. 5, March 1985, pp. 955-978.

17. Personal observations made by the author over the years in the field and participant observation conferences in the United States and abroad.

18. An early form of these kinds of activities was championed by Hacktivisimo, an offshoot of the Cult of the Dead Cow hacking group that developed a number of schemas that helped citizens get around Internet restrictions and avoid surveillance by repressive government regimes. There was some concern about using the software, as there were rumors that the software itself was a

security risk. For a more current example of this, see Associated Press (AP), "Chinese anti-censorship group Greatfire.org suffers massive hack," *The Guardian,* March 20, 2015, available from *www.theguardian.com/technology/2015/mar/20/chinese-anti-censorship-group-greatfire-org-suffers-massive-hack-google*, accessed September 9, 2015.

19. Sean Bodmer, Max Kilger, Gregory Carpenter, and Jade Jones, *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, New York: McGraw-Hill, 2012.

20. Nancy Whittier, "The Consequences of Social Movements for Each Other," in David A. Snow, Sarah A. Soule, Hanspeter Kriesi, eds., *The Blackwell Companion to Social Movements*, Oxford, UK: Blackwell Publishing, 2004, pp. 531-552.

21. Bill Maurer, "The Anthropology of Money," *Annual Review of Anthropology*, Vol. 35, September 21, 2006, pp. 15-36.

22. Often it is the money mules themselves that are scammed when the financial instrument they deposit into their accounts and forward using their own funds are found to be fraudulent. Other schemes where individuals in one country forward merchandise purchased with stolen credit cards to individuals in other countries often suffer similar fates when they are not paid by the scheme organizers. See Melvin R. J. Soudijn and Birgit C. H. T Zegers, "Cybercrime and virtual offender convergence settings," *Trends in Organized Crime*, Vol. 15, Iss. 2-3, September 2012, pp. 111-129.

23. Holt; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Santa Monica, CA: Rand Corporation, 2014.

24. Sadia Afroz, Vaibhav Garg, Damon McCoy and Rachel Greenstadt, "Honor among thieves: A common's analysis of cybercrime economies," in *eCrime Researchers Summit 2013 (eCRS 2013)*, Proceeding of the 2013 APWG eCrime Researchers Summit, eCRS 2013, San Francisco, CA, September 17-18, 2013, Institute of Electrical and Electronics Engineers (IEEE) Computer Society, 2013.

25. For an overview of motivations for malicious online acts and actors, see Kilger, "Social Dynamics and the Future of Technology-Driven Crime."

26. Afroz, Garg, McCoy, and Greenstadt.

27. Ablon, Libicki, and Golay.

28. *Ibid*.

29. Dorothy E. Denning, "Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000.

30. See Jonathan Matusitz, "The Networks That Fight Cyberterrorist Networks," *Journal of Human Behavior in the Social Environment*, Vol. 23, Iss. 5, 2013, pp. 616-626; and Gerald-Mark Breen, "Examining Existing Counter-Terrorism Tactics and Applying Social Network Theory to Fight Cyberterrorism: An Interpersonal Communication Perspective," *Journal of Applied Security Research*, Vol. 3, Iss. 2, 2008, pp. 191-204.

31. See Lorraine Bowman-Grieve, "A Psychological Perspective on Virtual Communities Supporting Terrorist and Extremist Ideologies as a Tool for Recruitment," *Security Informatics*, Vol. 2, Iss. 1, Art. 9, December 2013, pp. 1-5; and Raphael Cohen-Almagor, "In Internet's Way: Radical, Terrorist Islamists on the Free Highway," *International Journal of Cyber Warfare and Terrorism*, Vol. 2, Iss. 3, Art. 4, July-September 2013, pp. 39-58.

32. Thomas Hegghammer, "Interpersonal Trust on Jihadi Internet Forums," in Diego Gambetta, ed., *Fight, Flight, Mimic: Identity Signalling in Armed Conflicts*, Oxford University Press, forthcoming, pp. 4-5.

33. Max Kilger, "The Emergence of the Civilian Cyber Warrior," in Tarek Saadawi, Louis H. Jordan, Jr., and Vincent Boudreau, eds., *Cyber Infrastructure Protection: Volume II*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2013.

34. Max Kilger, "The Psychology of Cyberviolence," in Carlos A. Cuevas and Callie Marie Rennison, eds., *The Wiley-Black-*

well Handbook on the Psychology of Violence, New York: Wiley-Blackwell, 2015.

35. Thomas J. Holt, Max Kilger, Lichun Chiang, and Chu-Sing Yang, "Exploring the behavioral and attitudinal correlates of civilian cyberattacks," in Martin Bouchard, ed., *Social Networks, Terrorism and Counter-terrorism: Radical and Connected*, London, UK and New York: Routledge, 2015.

36. For an interesting comparison of terrorist groups in antiquity versus cyberterrorists of today, see Jonathan Matusitz, "Similarities between terrorist networks in antiquity and present-day cyberterrorist networks," *Trends in Organized Crime*, Vol. 11, No. 2, June 2008, pp. 183-199.

PART III:

CYBER INFRASTRUCTURE SECURITY

CHAPTER 7

SMART GRID VULNERABILITY ASSESSMENT USING NATIONAL TESTBED NETWORKS

Ihab Darwish
Obinna Igbe
Tarek Saadawi

OVERVIEW[1]

Security is an essential way to promote safety, protection, and data privacy. Security in critical infrastructure is about making data available only to authorized and authenticated users and ensuring the reliability of a system's operation with confidentiality and integrity. It is a balance between having the right mix of policies, strategies, and tools to secure the environment. In this chapter, we will discuss the smart grid as part of the critical infrastructure of the energy sector, and we will assess various smart grid vulnerabilities and provide a better understanding of the threats associated with them. Using the Defense Technology Experimental Research (DETER) Laboratory network testbed environment, we will perform cyberattack scenarios and evaluate various vulnerabilities of smart grid protocols.[2] A defense-in-depth security approach is highly recommended as a requirement for Critical Infrastructure Protection (CIP) along with the need to ensure protection is enforced in all layers.

INTRODUCTION

Today's critical infrastructure involves both physical and cyber components, integrated using legacy systems and new technologies working together over a Transmission Control Protocol/Internet Protocol (TCP/IP) platform. Legacy supervisory control and data acquisition (SCADA) systems were initially designed to be isolated systems that had both dedicated and separate communication links and, therefore, physical and cybersecurity threats were never considered to be an issue.[3] High availability, controllability, and maintainability requirements of today's systems demand a much higher level of communication to exist among various smart grid automation components, like Intelligent Electronic Devices (IEDs).[4] Specifically, IEDs are designed to automate protection, control, monitoring, and metering of the smart grid systems in both peer-to-peer and client server implementation that communicate directly to SCADA supervisory and control systems.

Security, especially data integrity, in communication protocols is one of the most challenging research areas involving smart grids. Communication is not just about data transfer; it is about ensuring accuracy, integrity, and confidentiality to critical data. Smart grid systems are complex environments that facilitate an improved and an efficient two-way path of communication and power-handling capabilities (see Figure 7-1). This involves up-to-date technologies in areas such as power, communication, and renewable energy resources in order to achieve highly secure, reliable, economic, and environmentally friendly electric power systems.[5]

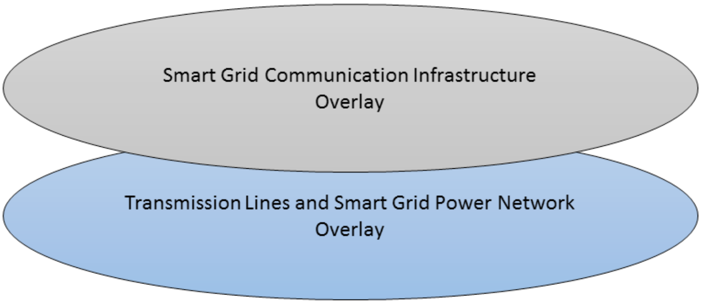

Smart Grid Communication Infrastructure Overlay
Transmission Lines and Smart Grid Power Network Overlay

Figure 7-1. Smart Grid Layers.

Several standards were developed over the years to provide communication within SCADA, such as MODBUS, Distributed Network protocol (DNP3), Process Field Bus (PROFIBUS), Inter-Control Center Communication protocol (ICCP), and the latest, the International Electrotechnical Commission 61850 (IEC 61850). DNP3, as our main focus in this research, is an Institute of Electrical and Electronics Engineers (IEEE)-1815 standard, and it is the primary protocol being deployed in smart grid systems and other utility providers.[6] It is considered to be the predominant SCADA protocol in the U.S. energy sector.

DNP3 is a reliable and efficient protocol operating in critical infrastructure environments, and it is used in the delivery of measurement data from an outstation or client located in the field to the master or server located at the control center. Therefore, it is very critical to study the protocol's behavior and its application in real-time implementation. According to "A Taxonomy of Attacks on the DNP3 Protocol," many deficiencies and vulnerabilities were identified in DNP3, including 28 generic attacks.[7] In our recent research, we modeled smart grid technology experimentally and theoretically to evaluate specific cybersecurity threats on DNP3; specifically, Man-in-the-Middle (MITM) attacks were explored and modeled using game theory analysis and techniques to provide an understanding of both detection and mitigation strategies.[8] Related SCADA attacks were also studied using different techniques, including fault trees, attack trees, and risk analysis that provided a more theoretical approach as opposed to our method that is more specific to DNP3 and based on experimental results to complement the conceptual analysis.[9]

The delivery of measurement data from an outstation or slave located in the field to a utility master operating in the control center is one activity that is established when control requests are made from the master to outstations by an operator or by using an automated process. Time synchronization, file transfer, and other related tasks between the master and the outstation occur and, therefore, it is very critical to study its behavior and application in real-time implementation.

Our approach consists of performing three primary tasks, starting with identification and testing of potential vulnerabilities associated with smart grid implementations involving DNP3. We will use smart grid testbed experiments on virtualization environments to analyze vulnerabilities and perform penetration testing using various types of attacks, including MITM, to identify possible threats associated with the smart grid. Ultimately, the use of an intrusion detection system (IDS) will be necessary to identify attackers targeting different parts of the smart grid infrastructure, and mitigation strategies will ensure a healthy check of the network.

Our research will have four primary objectives as follows:

- Review the critical infrastructure related to the energy sector and the smart grid technology.
- Assess security policies and strategies in the smart grid including the defense-in-depth security model.
- Evaluate smart grid threats, vulnerabilities and risk management, and mitigation strategies.
- Assess vulnerabilities and threats in DNP3 based smart grid infrastructures and perform attack experiments to show vulnerabilities using DETER as an example of the national testbed environment.[10]

Section two of this chapter will discuss critical infrastructures and smart grid technology. Security policies and procedures will be presented in section three. Overview of vulnerabilities and threats will be highlighted in section four, and examples of national testbed environments will follow in section five. In section six, we will demonstrate DNP3 attack experiments using DETER, followed by our conclusion.

CRITICAL INFRASTRUCTURE

Critical infrastructure is a collection of systems and assets both tangible and non-tangible that provide critical services to the nation (see Figure 7-2), and its protection must be addressed to ensure reliability and continuity to vital services in the health, energy transportation and other sectors. In this chapter, we will address the energy sector and evaluate the security aspects in electrical smart grids.

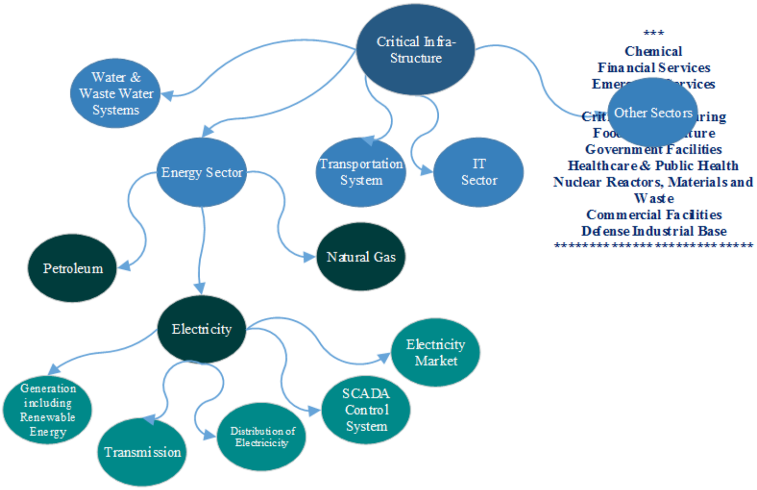


Figure 7-2. Critical Infrastructure—Energy Sector.

According to the U.S. Department of Homeland Security (DHS), more than 80% of the U.S. energy infrastructure is owned and operated by private sectors providing different kinds of energy sources including electricity, petroleum, and natural gas to households and businesses.[11] There are more than 6,400 power plants, 30,000 substations, and 200,000 miles of transmission lines in the nation. Vulnerabilities in this sector exist that demand the proper balance between using security protection technologies and enforcing security policies and procedures to protect nationwide assets. Reliability and business continuity is necessary for critical infrastructure implementations and, hence, cybersecurity is an essential aspect of this protection.

What is Smart Grid?

Smart grid was initiated by the National Institute of Standards and Technology (NIST), according to the American Recovery and Reinvestment Act (ARRA) in 2009, in order to establish intelligence and interoperability that incorporates smart technologies with various electricity distribution facilities and systems in order to improve the reliability of the grids.[12]

Smart grid is a collection of micro-grids interconnected and linked to the SCADA operating at the control center. Figure 7-3 depicts a smart grid where each micro-grid has the capability of operating independently or as part of the smart grid. Disconnection and micro-grid isolation is possible in case of hazards or blackout. Several measurement areas can be performed in each micro-grid, including power conditioning, time synchronization, validation, metering and others.

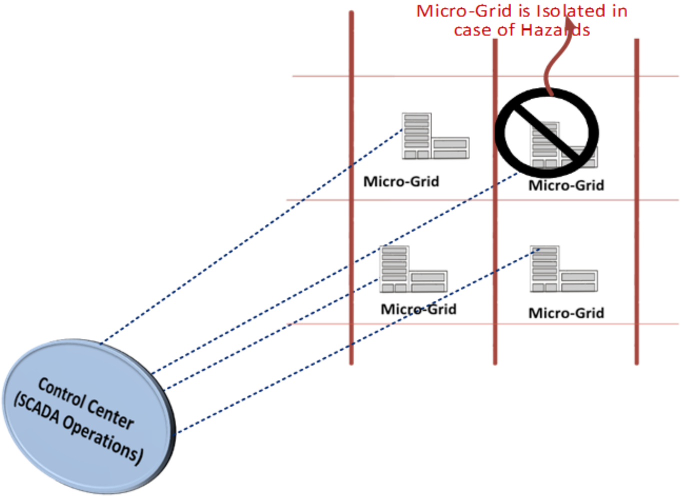

Micro-Grid is Isolated in case of Hazards
Micro-Grid
Micro-Grid
Micro-Grid
Micro-Grid
Control Center (SCADA Operations)

Figure 7-3. Critical Infrastructure—Smart Grid.

Smart grid systems are complex environments that facilitate an improved and an efficient two-way path of communication and power handling capabilities. This involves up to date technologies in areas such as power, communication, and renewable energy resources in order to achieve a highly secure, reliable, economic, and environmentally friendly electric power system. Smart grid as a critical infrastructure involves the deployment of smart meters at the remote sites connected via wireless communication and the Internet and managed directly by SCADA monitoring and control systems.

According to the Energy Sector Specific Plan, smart grids were initially modeled by NIST based on seven domains including customers, markets, service providers, operations, generation, transmission, and distribution.[13] That is a collection of complex technologies working together for the purpose of controlling demand and supply, managed directly by SCADA.

Smart Grid Communication Protocols.

Smart grid communication infrastructure is a part of the energy sector that utilizes many SCADA internal and external protocols in delivering control messages and monitoring data across different parts of the grid. Such data are being transported using one or more of the most popular SCADA protocols, including MODBUS, DNP3, and IEC 61850, in addition to the ICCP acting as the inter-master communication protocol.

MODBUS Protocol.

MODBUS protocol is an industrial standard that is used extensively in SCADA operations and is considered to be a popular one since its development back in

1979. MODBUS protocol has two versions for packet transmissions, serial and TCP versions. The protocol defines function codes and the encoding scheme for transferring data either as single points (1-bit, coils) or as 16-bit data registers. This basic data packet is then encapsulated according to the protocol specifications for MODBUS serial or TCP.

The TCP version of MODBUS follows the Open System Interconnection (OSI) model and defines the presentation and application layers as a master/slave protocol, meaning a device operating as a master will poll one or more devices operating as a slave. The master will write data to, and read data from, a slave device's registers. A register address or register reference is always in the context of the slave's registers.

Distributed Network Protocol (DNP3).

DNP3 is an open standard that can be deployed using several topologies, including: point-to-point (one master and one outstation or slave), multi-drop topology (one or multiple masters and multiple outstations), or the hierarchical layout where systems are arranged in a tree-like setup and one outstation could act as both a slave to a DNP3 master or a master to other outstations.[14] DNP3 messages can be mapped to the upper layers of the OSI model and are based on three layers including data link, transport, and application layers.

The DNP3 data link frame consists of a fixed size, 10-byte long header block, block 0, followed by a 282-byte long data portion that is divided into 16-byte blocks, each block ending with two bytes as a cyclic redundancy check code. There is 1-byte control field in the header.

International Electrotechnical Commission 61850 (IEC 61850).

IEC 61850 is one of the most recent protocols with the specification for the design and configuration of substation automation, and it supports a comprehensive set of substation functions and rich features for substation communications. IEC 61850 uses a link-layer multicasting protocol—known as the Generic Object Oriented Substation Events (GOOSE) protocol—for transmitting timing-critical messages, such as substation events, commands, and alarms, within the power substation networks.

Inter-Control Center Communication Protocol (ICCP).

ICCP, also known as the standard IEC 60870-6, is one of the major smart grid operating protocols used to interconnect masters from different micro-grids. Figure 7-4 shows a smart grid using an ICCP link between two masters operating at separate micro-grids.

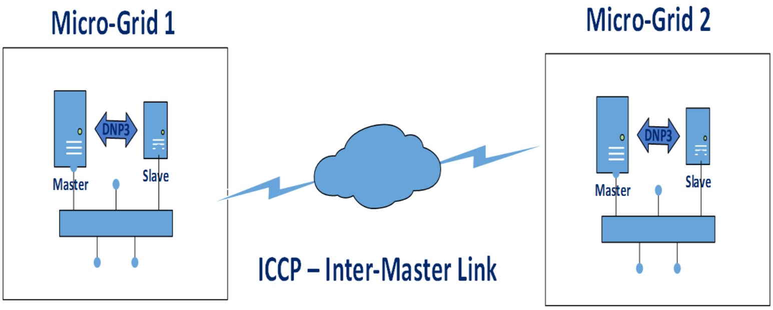


Figure 7-4. Smart Grid Communication.

The Internet paradigm, started in the mid-1990s, has played a major role in enabling the convergence between the conventional power grid and smart technologies. Reliable information transfer between smart grid components has become important to ensure performance, suitability, interoperability, and security. Therefore, we need to ensure smooth flow and secure transmission of traffic that will enable applications to manage power flow in the smart grid and to balance between the generation sources and the demands. Different asset sources and communication protocols are very important elements of the smart grid; over the years, there has been a tendency to standardize the protocols with enhanced security features.

SECURITY POLICIES AND STRATEGIES

A smart grid is comprised of several components, including power plant generators, distribution networks, micro-grids, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and smart meters located in remote areas. Additionally, there are control centers that are equipped with monitoring and control systems to oversee the entire operation of the smart grid.

Penetration starts with the weak security perimeter or layer as an entry point to all other layers (see Figure 7-5) in an attempt to reach the most critical part of the organization equipped with the highest security level. Weaknesses can be attributed to physical, cyber, or policy implementation, and attackers usually adopt certain penetration strategies when seeking specific information.

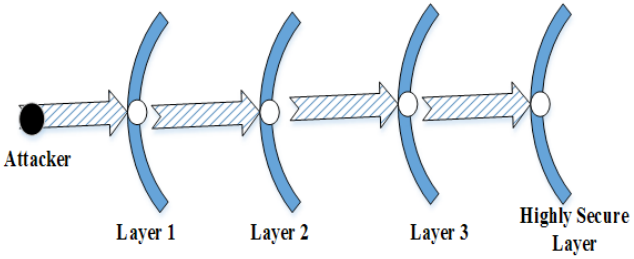


Figure 7-5. Critical Infrastructure Penetration.

Policies and Procedures.

Policies are rules established by organizations based on standards that are implemented by adopting a set of procedures and guidelines. Security policies in critical infrastructure, on the other hand, provide the strategy and the governing rules for guidance in protecting critical infrastructure components and valuable assets. The NIST—part of the U.S. Department of Commerce—is one of the organizations involved in smart grid infrastructure standards and policies. Figure 7-6 illustrates important organizations involved in critical infrastructure and related standards.

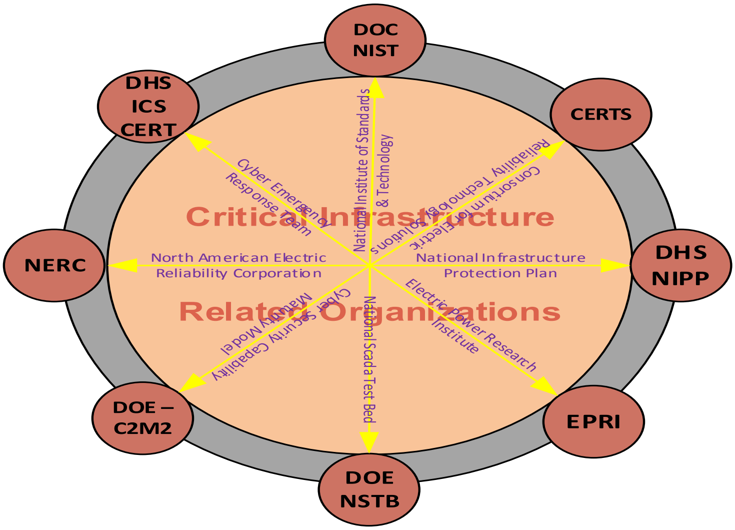

DOC NIST
DHS ICS CERT
CERTS
NERC
DHS NIPP
DOE – C2M2
DOE NSTB
EPRI
Critical Infrastructure
Related Organizations
Cyber Emergency Response Team
National Institute of Standards & Technology
Consortium for Electric Reliability Technology Solutions
North American Electric Reliability Corporation
National Infrastructure Protection Plan
Cyber Security Capability Maturity Model
National Scada Test Bed
Electric Power Research Institute

Figure 7-6. Critical Infrastructure—Related Organizations.

Security policies can be established at the enterprise level, and they can be issue-specific and/or system-specific policies. Security policies are implemented in order to ensure adherence to standards and safety measures, and in order to achieve the intended outcomes that are strategically set by the organization. Policies must be enforced in the organization, and there are several factors that must be considered in preparing proper policy:

- Policies should be applicable
- Polices should be enforced
- Empower users for policy adoption
- Policy auditing

An implementation of security policies and procedures must take into consideration the current and the future needs of the organization in order to promote stability, business continuity, and growth.

Strategies.

Strategy is defined as a set of activities that will be executed and aligned with a business's initiatives. In other words, we need to align the strategy with the business's success in order to have a healthy environment that could lead to growth and sustainability in the business. We also need to take into consideration the market competition and future growth in a dynamic environment and the open infrastructure in what is now called the Internet of Things (IoT).[15]

To address this topic from a cybersecurity prospective, we need to identify the organizational strategy for setting up security policies as well as how much investment is required to secure the infrastructure. In addition, we need to find an indication measure of the security using various parameters and baseline indicators to test the security level and its enforcement. Several models have been established in collaboration between different organizations to enforce security in an attempt to reduce risks associated with possible incidents on the smart grid.

In achieving our security goals and objectives, we need to have a mix of tools and initiatives in the form of policies and strategies to achieve the following:

- Adhere to all legal and legislative requirements and satisfy the U.S. Government's mandatory information management and security principles according to the information standards and guidelines.
- Develop, document, implement, and review information security controls.

- Ensure that smart grid infrastructure and information systems operate with a high degree of assurance and integrity.
- Protect assets and data both physically and logically from unauthorized or inappropriate use, accidental or fraudulent modification, and loss.

In pursuing these objectives, a defense-in-depth security strategy along with risk management framework and practices could be followed, in addition to internationally recognized governance principles and an adequate security framework.

The Defense-in-Depth Security Model.

A defense-in-depth security model is an enhanced practical strategy for achieving system reliability and information accuracy. It is a multilayer approach that uses technologies to balance protection, cost, performance, and operational capability.[16]

Protection using a defense-in-depth security model is handled through the application of multilayers of defense mechanisms. With an understanding of the organization's goals, the critical processes supporting these goals, and their interrelationships, the control structure surrounding the processes can be assessed. Controls will generally include both technical and process. Figure 7-7 provides a graphical representation of the layers of control implemented around a business process or key piece of business information, where data is the center of action or the core.

Most of today's organizations have invested in a variety of technologies for each layer of the OSI model, typically beginning with firewalls at the security perimeter, automated virus scanning technologies, physical security systems, spyware/adware detection software, automated or manual "patch" management, and other sophisticated network traffic monitoring and tracking tools. Figure 7-7 illustrates the five primary layers of the Defense-in-Depth Security Model. We have extended the model to include two additional foundation layers: Policies and Procedures as the first layer and Physical Security as the second layer.

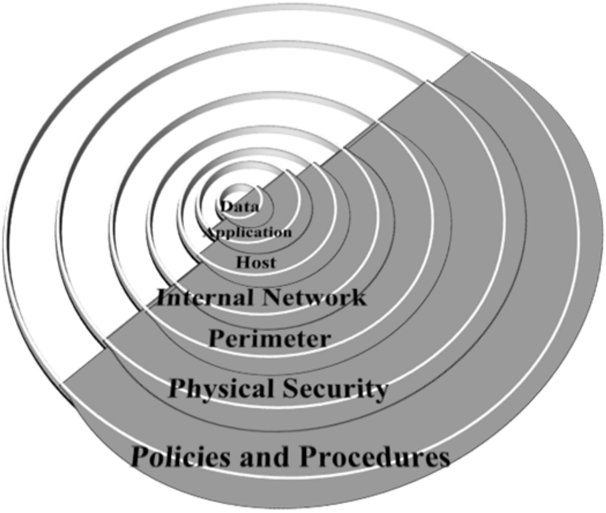


Figure 7-7. The Defense-in-Depth Security Model.

In recent years, it has become apparent that perimeter security as a security solution is not enough given the emerging trend, such as increased mobility and use of remote access, and increasing numbers of third parties accessing an organization's data and systems; the only effective mechanism for securing this information is via a layered defense-in-depth approach.

Identifying and justifying these types of technologies is an information technology (IT) manager's responsibility, but all managers involved and responsible for information security compliance should be kept apprised of the basics of technology so that they can participate in decisions about capital investments as part of an organizational approach to security management. Table 7-1 illustrates the different layers and the corresponding security device incorporated in that layer.

Layer	Defense Mechanism	Issues
First Layer **Policies and Procedures**	• Establish security policies • Enforce policies	• Organizational awareness issues • Policy auditing
Second Layer **Physical Security**	• Data centers and equipment control • Access control system	• Lack of physical security in remote locations
Third Layer **Security Perimeter**	• Firewalls, Virtual Private Network (VPN) encryption • Network-based Anti-Virus	• Vulnerable to attackers
Fourth Layer **Network**	• Network-based IDS • Vulnerability management systems • Network access control and User Authentication	• Could cause false alarms • Unauthenticated Access & Exploitation
Fifth Layer **Host**	• Host IDS • Host Anti-Virus	• Host based control, but limited to each device • New attacks are not detected
Sixth Layer **Applications**	• Public Key Interface (PKI) and Rivest, Shamir, and Adleman (RSA) algorithm • Access Control and Authentication	• Overhead and slow performance
Seventh Layer **Data**	• Encryption	• Good security but subject to security policies

Table 7-1. Extended Defense-in-Depth Security Layers.

VULNERABILITIES AND THREATS—SECURITY CONCERNS

A threat is anything that can cause an interruption to network operation or a system's functionalities and can jeopardize its availability. There are different categories of threats including natural threats like floods, earthquakes, storms, and unintentional accident types of threats. In addition, there are intentional threats that are caused by malicious intent. Each type of these threats can be catastrophic to a network. A vulnerability, on the other hand, is an open hole or fault susceptible to a threat attributed to intrinsic weakness in the design, configuration, or implementation of a network or system. Most vulnerabilities can usually be traced back to one of three major sources: poor design, poor implementation, or poor management.

Many vulnerabilities have been identified in smart grids employing SCADA control systems operating on different protocols. According to a DHS Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) monitor report, cyberattacks have increased from 9 in 2009, to 245 in 2014; and the reported number of incidents affecting various critical infrastructure is tabulated in Table 7-2, but the actual number could be much higher than what is indicated in the table.[17]

Year	Number of Incidents	% of Incidents in Energy Sector	Number of Vulnerabilities	Threat Activities Vector or Examples
2014	245	32%	159	• Unauthenticated Access & Exploitation • Buffer overflow • Spear Phishing • Network Scanning and probing • Structured Query Language (SQL) Injection • Unknown Access Vector (almost 50% of the cases)
2013	256	59%	187	
2012	198	41%	171	
2011	140	35%	138	

Table 7-2. Number of Incidents and Vulnerabilities.

In 2014, there were 159 known vulnerabilities in the control system, with the majority existing in the Energy Sector.

Attack and Penetration Strategy.

Attackers usually follow certain strategy or methodology to perform system attacks against the target network or host, similar to what is used by penetration testers as a sequential attack (see Figure 7-8). The steps involved in performing an attack include:

1. Reconnaissance or data gathering stage;
2. Scanning for potential target(s) and possible vulnerabilities;
3. Exploiting the vulnerability discovered in step 2; and,
4. Accessing the compromised host through logical connections.

Different tools are required in each of the stages mentioned above and most of the tools are available over the Internet with several unique ones being customized to serve a specific purpose. The methodology could include searching for vulnerabilities, performing sequential attacks, building an attack graph, and identifying weak points.

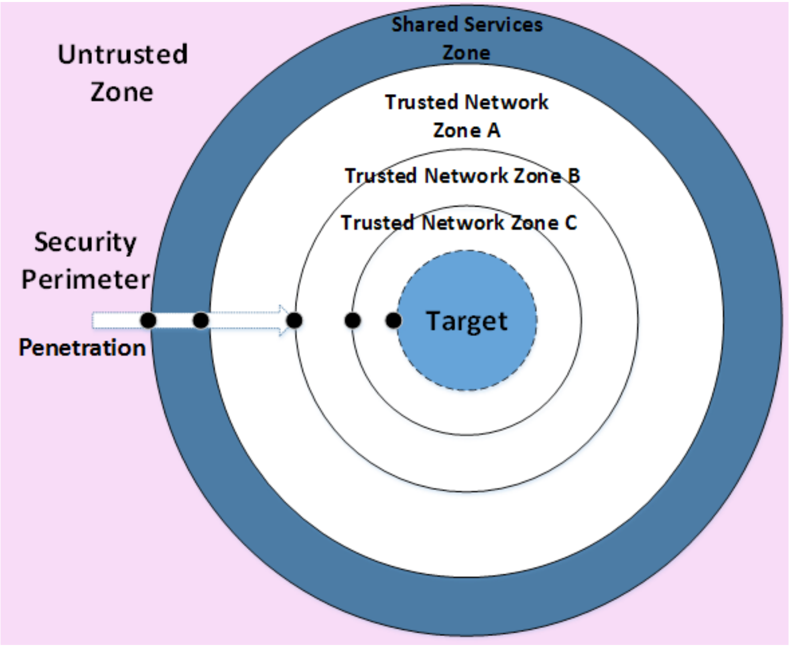


Figure 7-8. Penetration Strategy—Sequential Attacks.

Critical Infrastructure Security Concerns.

There are so many critical cybersecurity concerns that need to be addressed in critical infrastructure. Figure 7-9 shows some of the more pressing issues, including backdoors, protocol vulnerabilities, MITM, and many others.

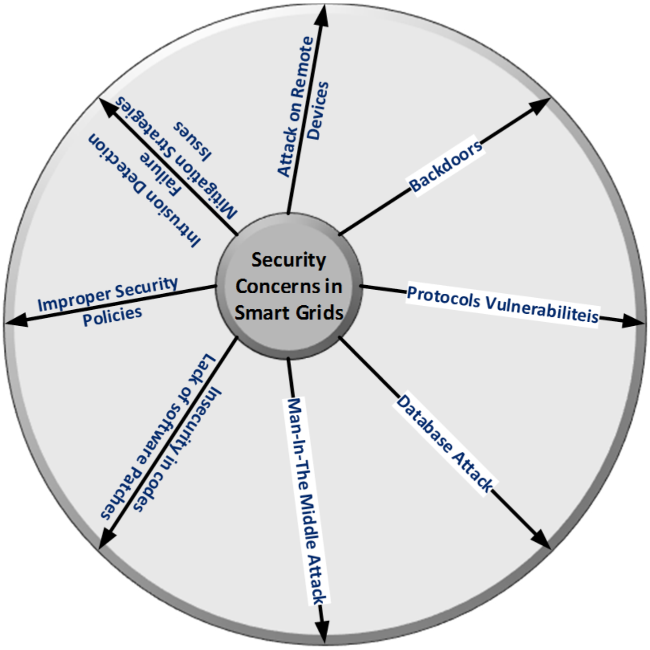
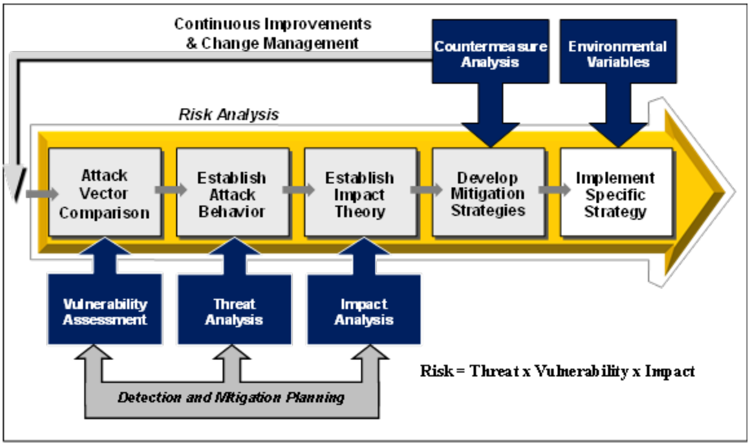

Security Concerns in Smart Grids
Attack on Remote Devices
Backdoors
Protocols Vulnerabiliteis
Database Attack
Man-In-The Middle Attack
Lack of software Patches
Insecurity in codes
Improper Security Policies
Intrusion Detection Failure
Mitigation Strategies Issues

Figure 7-9. Penetration Strategy—Sequential Attacks.

Risk Management.

Risk is the exposure to danger; risk management is the process of identifying vulnerabilities to an organization's infrastructure and assets in order to prepare mitigation strategies to eliminate or reduce the risk.[18] Therefore, risk management starts with risk identification to identify, classify, and prioritize threats, then moves to risk assessment to identify vulnerabilities and finally establish mitigation strategies to reduce or control the risk.

Risk is a function of three important variables: vulnerability, threat, and impact; and the risk will increase if any of those variables increases.[19] Therefore, in order to minimize the risk we need to know our threats in order to provide control measures to reduce the probability of having a vulnerability as a result of the threat. Figure 7-10 shows our framework in addressing risk management, starting with vulnerability assessment and followed by threat and impact analysis.



Continuous Improvements & Change Management
Countermeasure Analysis
Environmental Variables
Risk Analysis
Attack Vector Comparison
Establish Attack Behavior
Establish Impact Theory
Develop Mitigation Strategies
Implement Specific Strategy
Vulnerability Assessment
Threat Analysis
Impact Analysis
Risk = Threat x Vulnerability x Impact
Detection and Mitigation Planning

Figure 7-10. Risk Management.

According to the *National-Infrastructure-Protection-Plan* (NIPP) and the *Energy Sector-Specific Plan* (ESSP), both address the security and resilience in critical infrastructure through collaboration between private, non-profit organizations, and other U.S. Government sectors.[20] Objectives are related to prioritizing goals, mitigating risks, measuring progress and adapting to environmental changes. Physical, cyber, and human are the three elements of a critical infrastructure risk-management framework, and the framework is based on five phases as follows:

1. Set Goals and Objectives
2. Identify Infrastructure
3. Assess and Analyze Risks
4. Implement Risk Management Activities
5. Measure Effectiveness

NATIONAL TESTBED ENVIRONMENTS

Testbeds are essential platforms for the rigorous and replicable testing of theories, computational tools, new technologies, and systems. The testbed provides a development environment without the potential hazards or consequences present when testing in a live production environment. A testbed can be used to demonstrate new components or entire systems, and can include software and hardware/physical equipment as well as networking components.

With increased smart grid complexity, experimental studies of large-scale grids are usually not economically feasible, even for a small micro-grid environment with a limited number of distributed energy sources and intelligent loads. Only a few testing platforms around the world have been established.[21] Therefore, testbeds, simulation, virtualization, and theoretical modeling become powerful and convenient tools in this research area. The NIST, in its recent publication, listed a number of popular National SCADA Test Bed (NSTB) environments in the United States and their application in smart grids.[22]

Several examples of testbeds were created by both the government and the private sector, providing a natural resource to help improve the protection of critical infrastructure, system monitoring, and control. They provide great benefits to utility providers, vendors, and the research and development community for testing all aspects of the infrastructure that can speed up the research and development in networking and cybersecurity areas.

National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB).

Multiple national smart grid laboratories, as part of NSTB, include: Idaho National Lab, Sandia National Lab, Argome National Lab, Pacific Northeast Lab, and Oak Ridge Lab. Working in these testbeds will enable us to identify, assess, and mitigate current vulnerabilities and develop risk mitigation strategies and awareness programs though training.

Smart Grid System Testbed Facility.

The NIST Smart Grid Testbed Facility initiated a project to have a total of eight labs supporting dedicated NIST measurement science projects. The labs will be interacting with each other using several key measurement areas with the objective of accelerating the research and development of smart grid standards and interoperability with various micro grids.

Defense Technology Experimental Research (DETER) Lab Testbed Environment.

DETER lab is a testbed based on Emulab that was funded by the National Software Foundation (NSF), DHS, and the Defense Advanced Research Projects Agency (DARPA), and is designed specifically for large-scale cybersecurity projects and research.[23] DETER lab provides an open, remotely accessible, shared-network research lab that includes networking resources, computing resources, and an expanding set of tools to construct experiments.

One of the primary objectives of setting up a testbed is to evaluate security by testing threats and vulnerabilities in critical infrastructure. In this chapter, DETER is used to demonstrate several attack scenarios on smart grids incorporating DNP3 in a master and outstation configuration.

ATTACK EXPERIMENTS USING DEFENSE TECHNOLOGY EXPERIMENTAL RESEARCH (DETER)

In order to demonstrate vulnerabilities in smart grids, we will set up a basic grid infrastructure in DETER lab. In this section, we will simulate an experiment of the smart grid environment involving one master and one outstation or slave (see Figure 7-11) for the purpose of investigating important vulnerabilities and possible insider attack scenarios using MITM. The attacker node is connected to the same network as the master and outstation node.

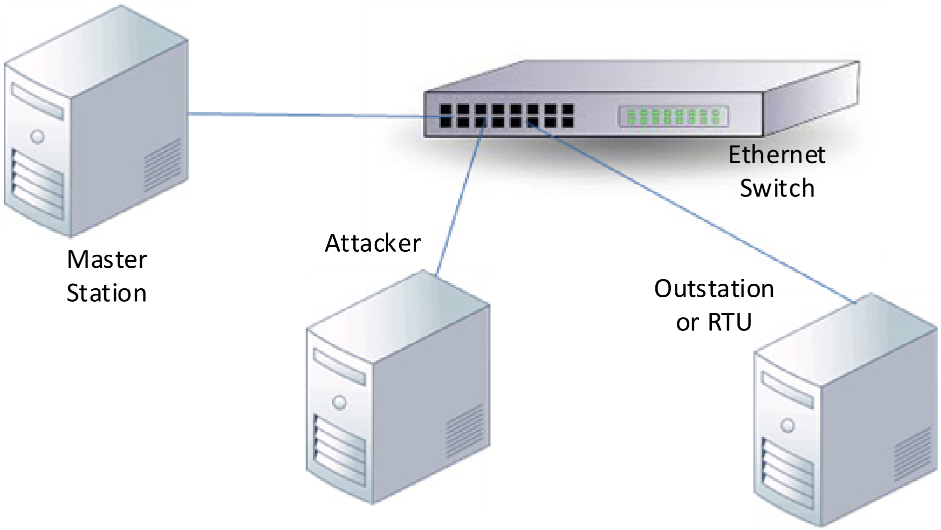


Figure 7-11. Insider Attack Scenario.

The master (M) and the outstation or slave (S) are both running an Ubuntu operating system with Open DNP3 protocol and are exchanging DNP3 request and response packets.[24] The attacker node (A) is also running Ubuntu, and with the help Ettercap tool, it is configured to be in the middle of the communication between the master and the outstation.[25] Now, to alter the exchanged packets between the master and the outstation, a new tool written in Python programming language was used to enable swift packet modification. The tool was able to capture only the DNP3 packets and Wireshark was used to validate this process.[26]

Attack Setup and Types in Distributed Network Protocol (DNP3).

To intercept the DNP3 packets, our first step would be to poison the slave and master node's Address Resolution protocol (ARP) cache by adding their IP address to Ettercap's target list for ARP poisoning. Several possible attack scenarios are implemented, as the following sections will show.

Man-in-the-Middle (MITM) Attack (Sniffing Slave and Master Generated Traffic).

MITM attacks can be categorized as network attacks, which can also form the basis for other types of attacks. In addition, there are many kinds of MITM attacks that exist, but we will be using the one that involves poisoning the ARP cache of the victims called ARP spoofing or poisoning. To perform this attack, the first requirement will be to have the attacker on the same network as the victims. Here, the attacker uses Ettercap, a network attack tool, to accomplish this attack by running the following code in the attacker node:

```
sudo ettercap -T -q -i eth3  -M ARP /10.1.1.2/ /10.1.1.3/
```

Where:

- "–T" option indicates that we intend to run the text-only version of Ettercap;
- "–q" means to run in quite mode;
- "-i" specifies the interface to be used (to get this interface i.e. eth3, first run the IP route to get 10.1.1.3); and,
- "-M" indicates that we will be running a MITM attack using an ARP poisoning technique.

With the above poisoning technique, the IP 10.1.1.2 and 10.1.1.3 specifies the victims (the master and the outstation node in this case). Hence, any traffic passing through LAN0 to and from the master or the outstation node would go through the attacker's machine. Figure 7-12 depicts the MITM attack performed on the attacker node (node B) against the victim node (node C); the traffic to and from node C passes through node B. If this attack is achieved, then the attacker can go further to perform other kinds of attacks against node C.

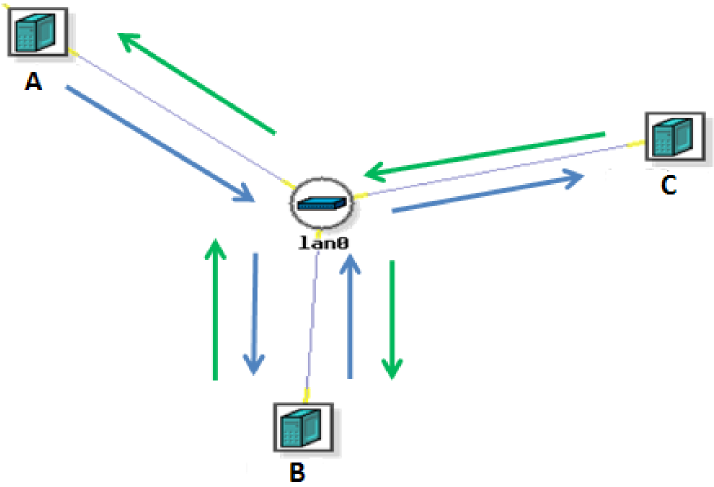


Figure 7-12. Traffic Flow During a Man-in-the-Middle (MITM) Attack.

Prior to the attack, Figure 7-13 shows that the traffic from the master or the outstation is not passing through the attacker node. The attacker's (with media access control [MAC]: 00:15:17:1e:05:2e) screen is shown in Figure 7-14 sending the ARP reply to the outstation node (IP: 10.1.1.3 and MAC: 00:15:17:1e:03:3e). Hence, the outstation node now thinks that the master node (IP: 10.1.1.2 and MAC: 00:15:17:1e:03:b0) can be reached by the address 00:15:17:1e:05:2e, which is the attacker's physical address. The attacker does a similar thing to the master node ARP table; this makes the master believe that the attacker node is the outstation.

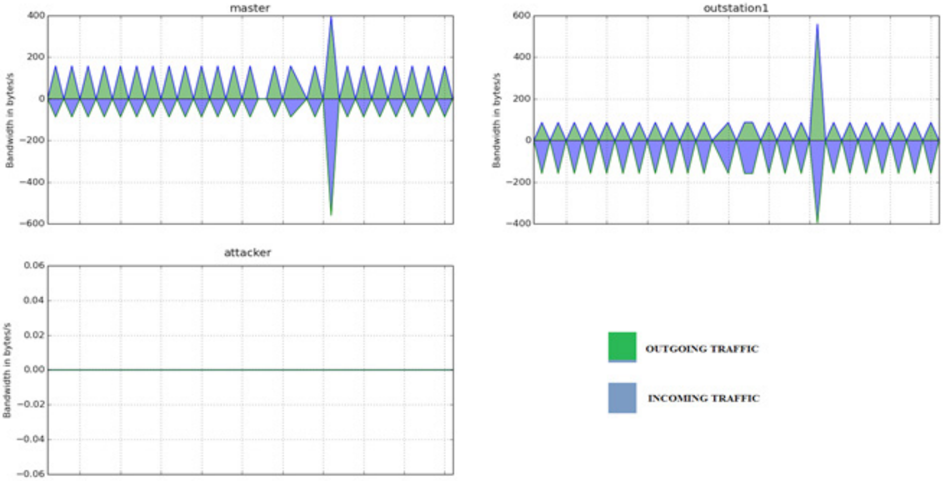
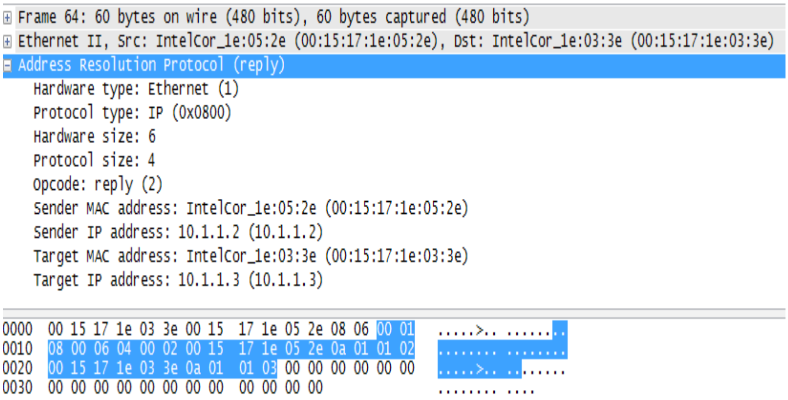


Figure 7-13. DNP3 Traffic Exchanged between Master and Outstation Not Passing Through the Attacker Node—Before ARP Poisoning.



```
⊞ Frame 64: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: IntelCor_1e:05:2e (00:15:17:1e:05:2e), Dst: IntelCor_1e:03:3e (00:15:17:1e:03:3e)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: IntelCor_1e:05:2e (00:15:17:1e:05:2e)
    Sender IP address: 10.1.1.2 (10.1.1.2)
    Target MAC address: IntelCor_1e:03:3e (00:15:17:1e:03:3e)
    Target IP address: 10.1.1.3 (10.1.1.3)

0000  00 15 17 1e 03 3e 00 15  17 1e 05 2e 08 06 00 01   .....>.. ........
0010  08 00 06 04 00 02 00 15  17 1e 05 2e 0a 01 01 02   ........ ........
0020  00 15 17 1e 03 3e 0a 01  01 03 00 00 00 00 00 00   .....>.. ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Figure 7-14. Address Resolution Protocol (ARP) Poisoning.

The poisoned ARP table of the outstation is shown below:

Before the attack:

```
user@outstation:~$ arp -a
attacker-lan0 (10.1.1.7) at 00:15:17:1e:05:2e [ether] on eth1
master-lan0 (10.1.1.2) at 00:15:17:1e:03:b0 [ether] on eth2
```

After the attack:

```
user@outstation:~$ arp -a
attacker-lan0 (10.1.1.7) at 00:15:17:1e:05:2e [ether] on eth1
master-lan0 (10.1.1.2) at 00:15:17:1e:05:2e [ether] on eth
```

Now, Figure 7-15 shows the bandwidth per second plotted before, during, and after performing the MITM attack. DNP3 traffic is now passing through the attacker node.

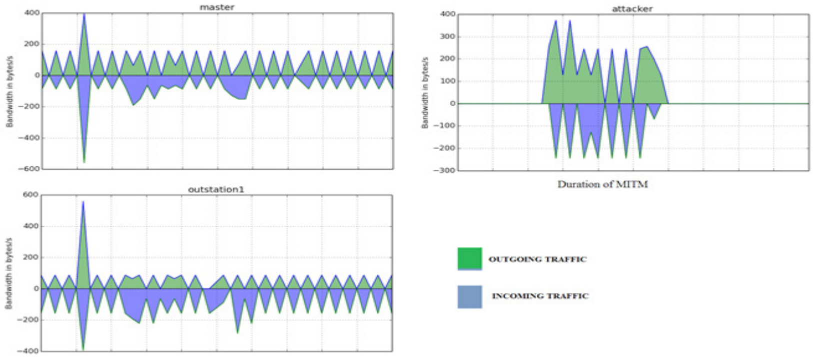


Figure 7-15. Master and Outstation DNP3 Traffic Passing Through the Attacker Node During the Duration of an MITM Attack.

Blackhole Attack (Packet Drop Attack) and Selective Distributed Network Protocol (DNP3) Packets Dropping Attack.

A packet drop attack or blackhole attack is considered to be a type of Denial of Service (DoS) attack in which all packets passed through the attacker are discarded instead of passing through to reach their destination. In a packet-dropping attack, packets are routinely and selectively dropped, making them very hard to detect and prevent.

If packets are selectively dropped, then this type of attack is called a gray-hole attack. To perform this attack, a python script is executed by the attacker node after a successful MITM attack. This script contains the following lines:

```
if(ip.src ==’10.1.1.2’ || ip.dst ==’10.1.1.2’):
    if (ip.proto == TCP && tcp.dst == 20000):
      drop()
       print (“DNP3 packet to or from Master node dropped\n”)
```

This code tells the attacker‘s interface to drop all DNP3 packets to and from the master node. To drop the packets to and from the outstation, the following lines are used:

```
if(ip.src =='10.1.1.3' || ip.dst =='10.1.1.3'):
    if (ip.proto == TCP && tcp.dst == 20000):
    drop()
    print ("DNP3 packet to or from Outstation node dropped\n")
```

The script identifies the DNP3 packets by looking for TCP packets that have a port number of 20000, which is the DNP3 port number. Figure 7-16 below shows the traffic before and after the attack.

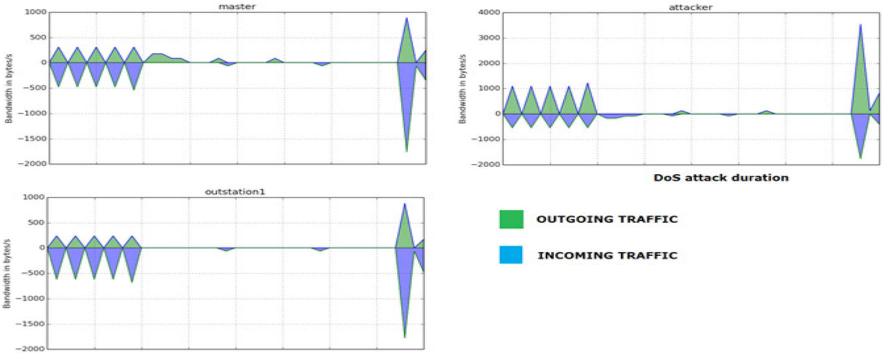


Figure 7-16. The Outstation Node Experiencing a Denial of Service (DoS) Attack.

From the Figure 7-16 above, the DNP3 packets (initial green traffic above the 0 line in the master graph) were sent out before the attack. However, during the attack, only non-DNP3 related TCP packets were allowed to pass through (the little green traffic above the 0 line). The outstation graph shows no response was made by the outstation. Notice that after the attack was completed, there was a sharp rise in the outgoing traffic at the outstation to send all the pending updates that occurred during the attack.

Distributed Network Protocol (DNP3) Packets Modification and Injection Attacks.

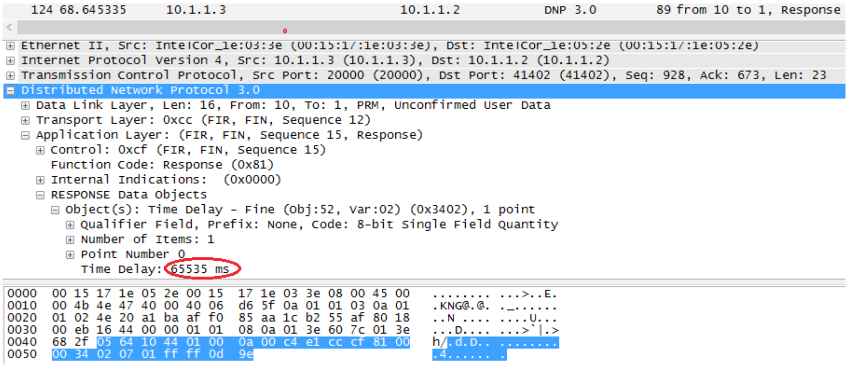
To manipulate or modify the DNP3 packets, we created a code to:

- Capture a packet instance and check the length of the TCP before modification;
- Replace the contents of the payload with the modified one;
- Get the new length of the TCP packet, payload and compute the difference in length between the new and the old;
- Set the new IP length field;
- Delete both of the IP and TCP checksum fields so the Scapy would recalculate this; and finally,
- Accept and forward the modified packet.[27]

To make all the modifications stated in the preceding sentence, we push the desired DNP3 payload to our attack code using the "nfqueue" python module in combination with Linux "iptables" utility that can be used to allow or to block incoming or outgoing traffic on specific ports. This code also predicts the sequence and acknowledgment numbers of the next packet to be sent by the victim node(s). This will enable the code to hijack the TCP connection later.

In order to inject the modified packet, the predicted sequence and acknowledgement numbers, as explained in the previous paragraph, are used to hijack the TCP connection. Then, Scapy is used to inject a malicious TCP packet to the already existing TCP connection. Hence, the slave would think that this crafted message came from a legitimate master. The test results showed that the attacker, by modifying the TCP/IP header and DNP3 messages, was able to manipulate, control, and redirect the DNP3 traffic and even change the exchanged messages (DNP3 payload) between the master station and the outstation.

Cold Restart Attack Example. When a DNP3 "Cold Restart" request command is received by the outstation and the packet is confirmed to have originated from the master, the outstation then performs a full restart on completion of the communications sequence. The outstation will also send a reply to the master with the time the outstation is available before restart. Figure 7-17 shows an example of this packet that was seen by Wireshark.



```
   124 68.645335      10.1.1.3                   10.1.1.2           DNP 3.0         89 from 10 to 1, Response
⊞ Ethernet II, Src: IntelCor_1e:03:3e (00:15:17:1e:03:3e), Dst: IntelCor_1e:05:2e (00:15:17:1e:05:2e)
⊞ Internet Protocol Version 4, Src: 10.1.1.3 (10.1.1.3), Dst: 10.1.1.2 (10.1.1.2)
⊞ Transmission Control Protocol, Src Port: 20000 (20000), Dst Port: 41402 (41402), Seq: 928, Ack: 673, Len: 23
⊟ Distributed Network Protocol 3.0
  ⊞ Data Link Layer, Len: 16, From: 10, To: 1, PRM, Unconfirmed User Data
  ⊞ Transport Layer: 0xcc (FIR, FIN, Sequence 12)
  ⊟ Application Layer: (FIR, FIN, Sequence 15, Response)
    ⊞ Control: 0xcf (FIR, FIN, Sequence 15)
      Function Code: Response (0x81)
    ⊞ Internal Indications:  (0x0000)
    ⊟ RESPONSE Data Objects
      ⊟ Object(s): Time Delay - Fine (Obj:52, Var:02) (0x3402), 1 point
        ⊞ Qualifier Field, Prefix: None, Code: 8-bit Single Field Quantity
        ⊞ Number of Items: 1
        ⊞ Point Number 0
          Time Delay: 65535 ms

0000  00 15 17 1e 05 2e 00 15  17 1e 03 3e 08 00 45 00   ........ ...>..E.
0010  00 4b 4e 47 40 00 40 06  d6 5f 0a 01 01 03 0a 01   .KNG@.@. ._......
0020  01 02 4e 20 a1 ba af f0  85 aa 1c b2 55 af 80 18   ..N .... ....U...
0030  00 eb 16 44 00 00 01 01  08 0a 01 3e 60 7c 01 3e   ...D.... ...>`|.>
0040  68 2f 05 64 10 44 01 00  0a 00 c4 e1 cc cf 81 00   h/.d.D.. ........
0050  00 34 02 07 01 ff ff 0d  9e                        .4...... .
```

Figure 7-17. Response to the Cold Restart Packet.

Figure 7-18 shows the traffic during and after the attack. From the outstation graph, we see that after receiving the command (the longer blue bump on the outstation's outgoing traffic), the outstation waits for 65535ms and then performs a full restart. This full restart can be seen by the 0 incoming and 0 outgoing traffic in the outstation traffic graph. In addition, given the master was not the originator of these commands, the master still thinks that the outstation node is online, hence, it will continue to retransmit its previous commands before the outstation restarts.

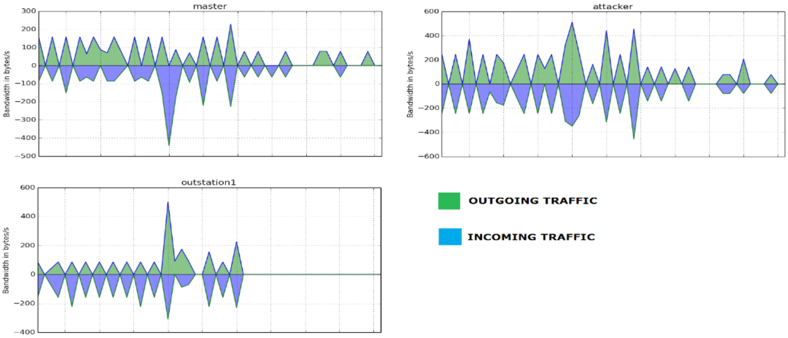


Figure 7-18. Outstation Restarting After Implementing the Cold Restart Command From the Attacker.

Unsolicited Messages Attack Example. Unsolicited messages are considered to be a way the RTU, or the outstation, can communicate certain activities or events data to the master station without being polled. Messages can be in the form of specific readings, warnings, or errors detected by the outstation that need to be sent to the master station for further and immediate actions. These messages are a way to ensure that current status is understood by the master station. For example, an unsolicited message from the RTU in a smart grid environment can be sent to the master, indicating the load's requirement has decreased, and it needs to be changed by the master station to a different value, and then the outstation will be expecting to receive the control message from the master.

In the virtualization environment, while normal communication is occurring between the master station and the outstation exchanging DNP3 messages encapsulated in TCP/IP packets, an attack is successfully performed to intercept the communication by stopping the outstation from sending unsolicited messages without affecting the normal communication behavior. Such an attack can lead to a very disastrous situation if such penetration occurred in the smart grid network. Figure 7-19 below shows an example of security penetration executed by the attacker to intercept the communication channel and to inject the malicious payload data without affecting the rest of the communication session.

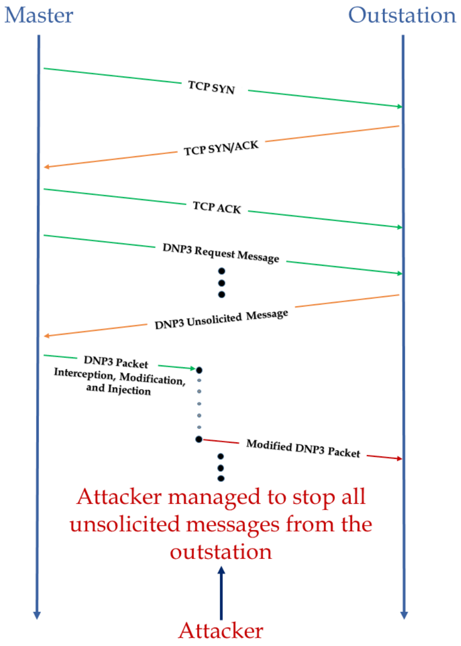

Master
Outstation
TCP SYN
TCP SYN/ACK
TCP ACK
DNP3 Request Message
DNP3 Unsolicited Message
DNP3 Packet Interception, Modification, and Injection
Modified DNP3 Packet
Attacker managed to stop all unsolicited messages from the outstation
Attacker

Figure 7-19. A Cyberattack Scenario—DNP3 Unsolicited Message Attack.

CONCLUSION

In order to minimize the impact of security attacks in smart grids as part of the critical infrastructure, our goal will be to minimize the frequency in which a smart grid is compromised, and to swiftly respond to minimize damage when a compromise occurs. There is no doubt that establishing a successful security policy requires investment. Moreover, the investment must take into consideration having the proper mix and balance between security products, polices, and strategies so that we can monitor and respond to attacks in a timely manner. Effective policies and strategies will depend on key performance indicators along with ensuring that all security layers are secured. In this chapter we modeled smart grid technology using several testing platforms including a virtual lab environment and DETER in order to evaluate specific cybersecurity threats and vulnerabilities on DNP3 operating in SCADA based implementation. We used various techniques in our analysis to setup different attack scenarios. Our contribution involved understanding critical infrastructure, DNP3 vulnerabilities in smart grids, and simulation using testbed platforms.

ENDNOTES – CHAPTER 7

1. An earlier version of this chapter appeared as the paper Ihab Darwish, Obinna Igbe, and Tarek Saadawi, "Smart Grid vulnerability Assessment Using National Testbed Networks," Presented at The City University of New York (CUNY), City College, Cyber Infrastructure Protection (CIP) Conference in New York on October 15, 2015.

2. DETER or DeterLab is the cyber-based Defense Technology Experimental Research Laboratory primarily used by researchers and academics as a testing bed to perform critical security experiments by emulating real-world complex scenarios with a high-level of scalability.

3. Jack Wiles, Ted Claypoole, Phil Drake, Paul A. Henry, Lester J. Johnson, Jr., Sean Lowther, Greg Miles, Marc Weber Tobias, and James H. Windle, *Techno Security's^{TM} Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure*, Burlington, MA: Syngress Publishing Incorporated, Elsevier, Incorporated, 2007; Gordon Clarke and Deon Reynders, *Practical Modern SCADA Protocols: DNP3, IEC 60870.5 and Related Systems*, Burlington, MA: Newnes, Elsevier, 2004.

4. Intelligent Electronic Devices (IEDs) are any station operating in a smart grid including a DNP3 master and outstation or slave; we use the terms "outstation" and "slave" interchangeably.

5. Richard E. Brown, "Impact of smart grid on distribution system design," in Proceedings of IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburg, July 20-24, 2008, pp. 1-4.

6. Ken Curtis, "A DNP3 Protocol Primer," DNP Users Group, March 20, 2005, available from *www.dnp.org/aboutus/dnp3%20primer%20rev%20a.pdf*; The Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard 1815-2012 (Revision of IEEE Standard 1815-2010)," *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*, October 10, 2012, p. 1,821.

7. Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi, eds., "A Taxonomy of Attacks on the DNP3 Protocol," in International Conference on Critical Infrastructure Protection (CIP), *Critical Infrastructure Protection III, IFIP Advances in Information and Communication Technology,* Vol. 311, Berlin: Springer, 2009, pp. 67-68.

8. Ihab Darwish, Obinna Igbe, and Tarek Saadawi, "Experimental and Theoretical Modeling of DNP3 Attacks in Smart Grids," *2015 36th IEEE Sarnoff Symposium: Proceedings of a meet-*

ing held 20-22 September 2015, Newark, New Jersey, USA, Institute of Electrical and Electronics Engineers (IEEE), 2015, pp. 155-160; Ihab Darwish, Obinna Igbe, Orhan Celebi, Tarek Saadawi, and Joseph Soryal, “Smart Grid DNP3 Vulnerability Analysis and Experimentation,” Paper Presented at the IEEE International Symposium of Smart Cloud, IEEE SSC 2015, on November 3, 2015, in New York.

9. Chee-Wooi Ten, Junho Hong, and Chen-Ching Liu, “ Anomaly Detection for Cyber Security of the Substations,” *IEEE Transaction on Smart Grid*, Vol. 2, No. 4, Dec. 2011.

10. The DETER Project website, available from *www.deter-project.org/*.

11. U.S. Department of Homeland Security, “Energy Sector,” January 19, 2016, updated January 12, 2017, available from *www.dhs.gov/energy-sector*.

12. National Institute of Standards and Technology (NIST), U.S. Department of Commerce website, available from *www.nist.gov/*; *American Recovery and Reinvestment Act of 2009*, Public Law 111-5, 111 Congress, 1st Session, January 6, 2009, available from *https://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf*.

13. U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010*, Washington, DC: U.S. Department of Energy and U.S. Department of Homeland Security, 2010, available from *http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf*.

14. DNP3 website, available from *www.DNP3.org*.

15. Ovidiu Vermesan and Peter Friess, eds., *Internet of Things: From Research and Innovation to Market Deployment*, Aalborg, DK: River Publishers, 2014.

16. “Information Assurance,” U.S. National Security Agency and U.S. Central Security Service website, May 4, 2016, available from *https://www.nsa.gov/ia/_files/support/defenseindepth.pdf*.

17. "The Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT)," U.S. Department of Homeland Security Official website, n.d., available from *https://ics-cert.us-cert.gov*.

18. Patricia A.S. Ralston, James H. Graham, and Jeffrey L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Transactions*, Vol. 46, No. 4, October 2007, pp. 583-94, published online July 10, 2007.

19. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, *Guide for Conducting Risk Assessments: Information Security*, NIST Special Publication 800-30, Rev. 1, Gaithersburg, MD: National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, September 2012, available from *nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.*

20. U.S. Department of Homeland Security, *NIPP 2013 Partnering for Critical Infrastructure Security and Resilience*, Washington, DC: U.S. Department of Homeland Security, 2013, available from *http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf*; U.S. Department of Energy and U.S. Department of Homeland Security, *Energy Sector-Specific Plan: 2015*, Washington, DC: U.S. Department of Energy and U.S. Department of Homeland Security, 2015, available from *https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.*

21. Robert H. Lasseter, Joseph H. Eto, Benjamin L. Schenkman, John Stevens, Harry T. Volkommer, Dave A. Klapp, Ed Linton, Hector H. Hurtado, Jean Roy, and Nancy Lewis, "CERTS Microgrid Laboratory Test Bed," *IEEE Transactions on Power Delivery*, Vol. 26, No. 1, January 2011, pp. 325–332.

22. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, *Measurement Challenges and Opportunities for Developing Smart Grid Testbeds: Summary Report*, Gaithersburg, MD: National Institute of Standards and Technology, December 2014, available from *http://www.nist.gov/smartgrid/upload/SG-Testbed-Workshop-Report-FINAL-12-8-2014.pdf*.

23. Emulab: total network testbed website, available from *http://www.emulab.net/*.

24. Ubuntu operating system, available from *www.ubuntu.com*; DNP3 (IEEE-1815) protocol, C++ with bindings for .NET and Java program, available from *https://github.com/automatak/dnp3*.

25. Ettercap program, available from *github.com/Ettercap/ettercap/issues/23*.

26. Wireshark program, available from *www.wireshark.org*.

27. Scapy program, available from *www.secdev.org/projects/scapy*.

ABOUT THE CONTRIBUTORS

HAIDAR CHAMAS is a Senior Consultant who is affiliated with the Center for Information Networking and Telecommunications (CINT) at the City College (CCNY) of the City University of New York (CUNY). He is also an adjunct professor at Florida Gulf Coast University in Fort Myers, FL. Dr. Chamas worked in academia for more than 10 years and for Verizon Communications for over 18 years. He was a manager of Internet and fast packet technology, director of product development and product management, and manager of systems integration and testing for securing broadband products and services as well as product security evaluations of network infrastructures.

LIEUTENANT COLONEL (LTC) JOHN D. COLWELL, JR. U.S. Army (Ret.) was the Deputy Director of Academic Engagement at the Strategic Studies Institute, U.S. Army War College, from 2012 until his retirement from the Army in 2014. While on active duty, his assignments included U.S. Forces-Afghanistan J-5 Plans, U.S. Army-Pacific G-5 Plans, and Assistant Professor, Department of Defense and Strategic Studies, United States Military Academy at West Point. LTC Colwell also served in various leadership roles as an infantry platoon leader in the 1st Infantry Division and as a company commander in the 25th Infantry Division (Light). He is a project manager with the multinational corporation ABB Inc., in the power generation and water operations division of North America. LTC Colwell holds a B.S. in history from West Point, NY, and an M.A. in diplomacy and military studies from Hawaii Pacific University.

IHAB DARWISH is a Ph.D. candidate in Electrical Engineering at the City College (CCNY) of New York. He is involved in cybersecurity research and affiliated with the Center for Information Networking and Telecommunications (CINT) at CCNY of the City University of New York (CUNY), where he has a research focus on network vulnerabilities, attack models, simulation, and prevention techniques covering different practical implementations including power-grid systems. He is a certified Project Management Professional (PMP) holding multiple certificates from the industry including Microsoft and Oracle with more than 20 years of information technology (IT) and project management related experience, and has worked with various IT solutions and applications in many different business environments. Currently, he is a visiting professor at DeVry University and a lecturer at various institutions in NY and NJ in the areas of electrical engineering and IT.

ADEL ELMAGHRABY is a professor and chair of the Computer Engineering and Computer Science Department at the University of Louisville. He has also held appointments at the Software Engineering Institute at the Carnegie Mellon University, and the University of Wisconsin-Madison. He received his B.S. from Alexandria University, Faculty of Engineering; a Graduate Diploma from Cairo University, Faculty of Economics; a Graduate Diploma from the Institute of National Planning, Egypt; and, an M.S. and a Ph.D. from the University of Wisconsin-Madison. He advised approximately 60 master's graduates and 25 doctoral graduates. His research contributions and consulting spans the areas of: Intelligent Multimedia Systems, Network and Information Security, Distributed Computing, Visualization, and Simulation. He is a well-published author (over 200 publications), a public speaker, member of editorial boards, and technical reviewer. He has been recognized for his achievements by several professional organizations including a Golden Core Membership Award by the Institute of Electrical and Electronics Engineers (IEEE) Computer Society (CS). He is a senior member of the IEEE. He served a term as an elected International Society for Computers and their Applications (ISCA) Board member and currently is a Senior Member and an Associate editor for the ISCA Journal. His activities on the IEEE-CS Technical Activities Board included chairing the finance committee, the simulation committee, and the emerging technologies initiatives. Dr. Elmaghraby's continued collaborations, mentoring, and scientific contributions have resulted in many presentations and published articles in prestigious journals such as *IEEE-TMI*, *Medical Physics*, *Journal of Neuroscience Methods*, and *Protein Engineering*. He is also the president of the Association of Egyptian-American Scholars (AEAS) and a proud Honorary Kentucky Colonel.

THOMAS HOLT is an associate professor in the School of Criminal Justice at Michigan State University specializing in cybercrime, cyberterror, and policy. He received his Ph. D. in criminology and criminal justice from the University of Missouri-Saint Louis in 2005. He has published extensively on cybercrime and cyberterror with over 40 peer-reviewed articles in outlets such as *The British Journal of Criminology*, *Crime and Delinquency*, and the *Journal of Criminal Justice*. Dr. Holt has also co-authored multiple books, including *Cybercrime and Digital Forensics: An Introduction* (Routledge), and *Policing Cybercrime and Cyberterror*

(Carolina Academic Press). He has also given multiple presentations on cybercrime and hacking at academic and professional conferences around the world, as well as hacker conferences across the country including Defcon and HOPE.

OBINNA IGBE is a Ph.D. candidate in the Department of Electrical Engineering at the City College of the CUNY. His research interests center around critical infrastructure protection (CIP), with a particular emphasis on smart grid network security. He is also working as a research assistant at the Center for Information Networking and Telecommunications (CINT) at the City College (CCNY) of the City University of New York (CUNY), where he is currently researching on the application an artificial immune system (AIS) to intrusion detection system (IDS) design.

ALEX KIGERL is an Assistant Research Professor of Criminal Justice and Criminology at Washington State University (WSU). Dr. Kigerl received his M.S. in criminology and criminal justice from Portland State University and his Ph.D. from WSU. His previous work was as a data analyst for the Washington State Institute for Criminal Justice (WSICJ), managing the criminal justice datasets and databases from partner state agencies in Washington for WSU researchers. His current work is focused on developing new risk assessment instruments for predicting criminal recidivism and re-hospitalization for the Department of Corrections and the Washington State Institute for Public Policy (WSIPP). His research interests include corrections, personality theory, and cybercrime with a focus on illicit email spam.

MAX KILGER has been the Director of the Data Analytics Programs of the College of Business since 2015, leading the college's initiative in big data. In addition, he is a faculty member in marketing and information systems and cybersecurity. He previously worked in industry as the chief behavioral scientist at Experian-Simmons. Dr. Kilger works in big data analytics from both digital and non-digital sources. He has two U.S. patents on methodologies related to big data and big data integration. He is a founding member of the Honeynet Project for cybersecurity; he is also a frequent national and international speaker for federal law enforcement agencies, military commands, and the intelligence community. He has published scholarly articles and books in the areas of marketing and cybersecurity. Dr. Kilger has won teaching awards at Stanford University and San Jose State University and has taught a wide variety of data related courses such as Research Methods, Marketing Research, and Internet and Society.

NIR KSHETRI is professor at Bryan School of Business and Economics, the University of North Carolina at Greensboro, and a research fellow at the Research Institute for Economics & Business Administration, Kobe University, Japan. Dr. Nir is the author of four books including *Cybercrime and Cybersecurity in the Global South* (Palgrave 2013), and *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (Springer-Verlag: Berlin, Heidelberg, New York). His 2014 book *Global Entrepreneurship: Environment and Strategy* (Routledge: New York) was selected as an Outstanding Academic Title by *Choice Magazine* (January 2015 Issue). Dr. Nir has also published 86 journal articles. Dr. Nir participated as lead discussant at the

Peer Review meeting of the United Nations Conference on Trade and Development's *Information Economy Report 2013* and *Information Economy Report 2015*. He is a two-time winner of the Pacific Telecommunication Council's Meheroo Jussawalla Research Paper Prize (2008 and 2010). Nir has been interviewed or quoted in over 60 TV channels, magazines, and newspapers.

MICHAEL LOSAVIO is an assistant professor in the Department of Criminal Justice at the University of Louisville; he also teaches in the Department of Computer Engineering and Computer Science on issues of law, society and information assurance in the computer engineering and justice administration disciplines. His focus is on law and social sciences as they relate to computer engineering and digital forensics. He holds a J.D. in law and a B.S. in mathematics from Louisiana State University. He lectured on computer law and crime at Perm State University, Russia, as a 2013 Fulbright Specialist.

TAREK SAADAWI is the director of the Center for Information Networking and Telecommunications (CINT) and a professor at the City College (CCNY) of the City University of New York (CUNY). Dr. Saadawi has published extensively in the area of information networks and network security. He is a co-editor of the books, *Cyber Infrastructure Protection: Volume 1* (Strategic Studies Institute, 2011), and *Cyber Infrastructure Protection: Volume 2* (Strategic Studies Institute, 2013), and the lead author of the book *Fundamentals of Telecommunication Networks* (John Wiley & Sons, 1994), which has been translated into Chinese. His most recent work has focused on network security, the vulnerability of wireless networks, denial of service (DoS) attacks and mitigation strategy, resilient routing protocols for ad-hoc wireless networks, connected vehicles security, and smart grid vulnerability analysis and its intrusion detection schemes.

U.S. ARMY WAR COLLEGE

Major General William E. Rapp
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Editors
Tarek Saadawi
John D. Colwell, Jr.

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil

U.S.ARMY

THE UNITED STATES ARMY WAR COLLEGE

STRENGTH and WISDOM

CUNY The City University of New York

the City College of New York

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT

armywarcollege.edu

ISBN 1-58487-753-7

9 781584 877530

90000>

This Publication

SSI Website

USAWC Website