NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PROTECTING NETWORKS VIA AUTOMATED DEFENSE OF CYBER SYSTEMS

by

Matthew E. Morin

September 2016

Thesis Co-Advisors:	Scott Jasper Ted G. Lewis

Approved for public release. Distribution is unlimited.

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

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

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE PROTECTING NETWORKS VIA AUTOMATED DEFENSE OF CYBER SYSTEMS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Matthew E. Morin	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

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

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Over the next ten to fifteen years, the number of internet-enabled devices is anticipated to grow exponentially, which will magnify cyber risks across an expanding attack surface area. It is unclear whether current manual methods of detection, verification, and remediation will allow network defenders to keep up with those risks. This thesis examined whether automated cyber defenses promise to be more effective than current models to cope with the results of vulnerabilities introduced by the projected increase in internet-enabled devices. The thesis further proposed a future model called Automated Defense of Cyber Systems, built upon three core technological components: sensors, autonomics, and artificial intelligence. Our conclusion is that automation is the future of cyber defense, and that advances are being made in each of the three technological components to support needed productivity gains for information technology security personnel. Continued advances will occur piecemeal, and it is recommended that network defenders make incremental investments consistent with an automated defensive strategy.

14. SUBJECT TERMS Internet of Things, autonomics, sensors, artificial intelligence, cyber defense, active cyber defense, automated indicator sharing, NIST cybersecurity framework, continuous diagnosis, mitigation	**15. NUMBER OF PAGES** 87
	16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

PROTECTING NETWORKS VIA AUTOMATED DEFENSE OF CYBER SYSTEMS

Matthew E. Morin
Supervisory Special Agent, Federal Bureau of Investigation
B.S., Oregon State University, 1992
MBA, University of Hawaii at Manoa, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2016

Approved by: Scott Jasper
Thesis Co-Advisor

Ted G. Lewis, Ph.D.
Thesis Co-Advisor

Erik Dahl, Ph.D.
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Over the next ten to fifteen years, the number of internet-enabled devices is anticipated to grow exponentially, which will magnify cyber risks across an expanding attack surface area. It is unclear whether current manual methods of detection, verification, and remediation will allow network defenders to keep up with those risks. This thesis examined whether automated cyber defenses promise to be more effective than current models to cope with the results of vulnerabilities introduced by the projected increase in internet-enabled devices. The thesis further proposed a future model called Automated Defense of Cyber Systems, built upon three core technological components: sensors, autonomics, and artificial intelligence. Our conclusion is that automation is the future of cyber defense, and that advances are being made in each of the three technological components to support needed productivity gains for information technology security personnel. Continued advances will occur piecemeal, and it is recommended that network defenders make incremental investments consistent with an automated defensive strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION..1
- A. BACKGROUND..2
- B. METHODOLOGY..4
- C. OVERVIEW..4

II. FUTURE LANDSCAPE OF CYBERSECURITY..7
- A. INTERNET OF THINGS IMPACT ON CYBERSPACE..7
  - 1. Exponential Growth..8
  - 2. IoT Impact on Cybersecurity..9
- B. IT SECURITY PERSONNEL AND BUDGETS..11
  - 1. IT Security Personnel..11
  - 2. IT Security Budgets..12
- C. MALICIOUS ACTORS..12
  - 1. Terrorism..13
  - 2. Nation States..14
  - 3. Organized Crime..16
- D. INCENTIVES AND FREQUENCY OF CYBER ATTACKS..17
  - 1. Cost to Attack..18
  - 2. Cost of an Attack..19
  - 3. Attack Frequency..19

III. CURRENT CYBERSECURITY EFFORTS..23
- A. A FEW WORDS ABOUT THE INTERNET..23
  - 1. Origins of Cybersecurity..23
  - 2. Inherent Insecurity..24
- B. DEFENSIVE MODELS..25
  - 1. Network Boundary Control..25
  - 2. Defense-in-Depth..26
  - 3. Continuous Monitoring..27
  - 4. Intelligence-Driven..29
- C. KEY CYBERSECURITY EFFORTS..31
  - 1. NIST Cybersecurity Framework..31
  - 2. Automated Indicator Sharing..33
  - 3. Continuous Diagnosis and Mitigation..34
  - 4. Active Cyber Defense..36

IV. AUTOMATED DEFENSE OF CYBER SYSTEMS 41
A. DEFINING ADCS..41
1. Automation 41
2. ADCS Core Components..42
B. SENSORS 43
1. The Sensing Device 43
2. Sensor Arrays..45
3. Data Collection and Aggregation 45
C. AUTONOMIC COMPUTING 46
1. Self-Configuring, Healing, and Optimizing...............................46
2. Self-Protecting...47
D. ARTIFICIAL INTELLIGENCE...49
1. Machine Learning...49
2. Situational Awareness 50
3. Dealing with Uncertainty 51
4. Human Analogy 51

V. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS 53
A. FINDINGS 53
B. CONCLUSIONS 54
C. RECOMMENDATIONS...54
D. FUTURE RESEARCH..55

LIST OF REFERENCES 57

INITIAL DISTRIBUTION LIST 67

LIST OF FIGURES

Figure 1. Projected Number of IoT Devices 8

Figure 2. OWASP Top10 IoT Vulnerabilities in 2014 10

Figure 3. Projecting Federal Cyber Incidents Reported to US-CERT 21

Figure 4. CREST Monitoring and Logging Framework 28

Figure 5. Deloitte Cyber Intelligence Model..30

Figure 6. NIST Cybersecurity Framework Tiers and Functions 32

Figure 7. CDM Operational Model 35

Figure 8. NSA/IAD’s ACD Conceptual Architecture..37

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACD	Active Cyber Defense
ADCS	automated defense of cyber systems
AI	artificial intelligence
AIS	Automated Indicator Sharing
ANS	Artificial Narrow Intelligence
BLS	Bureau of Labor Statistics
CCTV	closed-circuit television
CDM	Continuous Diagnosis and Monitoring
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
IAD	Information Assurance Directorate
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
NIST	National Institute of Standards and Technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OWASP	Open Web Application Security Project
PII	personally identifiable information
PRC	People’s Republic of China
PwC	PricewaterhouseCoopers

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis examined if automated cyber defense promises to be more effective than current models to cope with the results of vulnerabilities introduced by the projected increase in internet-enabled devices. The question was scoped to foresee cyberspace landscape evolution over the next 10 to 15 years. In particular, the author claims the anticipated exponential growth of internet-of-Things (IoT) devices will open vulnerabilities at such a rate that current manual methods of detection, verification, and remediation will not be able to keep up. The thesis then explains why the automation of cyber defenses will be more effective than current models in performing methodical tasks, and that such automation will be required to handle the oncoming crush of IoT devices and associated vulnerabilities.

Current defensive models and efforts are not adequate to defend networks from the volume of vulnerabilities introduced through IoT devices. Three gaps contribute to this: 1) the expected exponential growth of IoT devices, 2) limited growth of IT security personnel and budgets, and 3) an increase in cyber attacks, to include machine-to-machine attacks. The mass proliferation of internet-enabled devices has the potential to unravel traditional mechanisms of coping with cyber attacks. The Federal Bureau of Investigation (FBI) has warned of threats associated with the spread of IoT devices, and the number of attacks are increasing. The compromise of vulnerable devices connected to the internet will foster malicious actor attempts to disrupt or gain access to all types of sensitive networks. Furthermore, the number of cybersecurity professionals will not grow at the same pace as the devices requiring protection. This will result in expanding gaps in cyber defenses.

The IoT wave began in earnest in the early part of the current decade, and there is no reason to believe it will abate from exponential growth. Additionally, the internet has shown to be inherently insecure since inception, with new vulnerabilities introduced and identified on a regular basis. Terrorism, nation states, and organized crime will continue to be the primary malicious actors, and the level of associated threat may even grow as the cost to conduct offensive cyber operations drops while the cost to defend increases.

Consequently, there will be a greater surface area with vulnerabilities exploitable by those motivated to attack.

Defensive models have evolved since the inception of the internet, beginning with a simplistic exterior network defense, progressing to layered, ever-vigilant, and intelligence driven. Both industry and government have adapted to increasingly complex networks, setting frameworks for establishing defensive efforts, exchanging attack intelligence, and moving toward partial automation. However, broad use of external/ offensive cyber operations is not viable, particularly by private industry, as it has high business and professional risks, introduces the potential for criminal liability, and may lead to unintended escalation between nation states.

Greater automation is viewed as the future of cyber defense. Numerous technological advantages are on the near-to-mid horizon to help perform many cybersecurity functions. They will take advantage of the same exponential growth curve as seen in the introduction of IoT devices, thereby allowing a slowly growing number of cybersecurity professionals to defend vastly larger and more complex networks. Three core technological components are identified as essential toward realizing what is proposed by the thesis as the automated defenses of cyber systems (ADCS): sensors, autonomic computing, and artificial intelligence (AI). Various technological advancements are cited as evidence of each component's emergence.

The realization of ADCS will not take place overnight. It is much more likely it will arrive piecemeal, with incremental improvements to the sensor, autonomic, and AI components. National policy should continue to encourage investment in the broad use of defensive cyber automation. Such automation should be limited to activities contained within a defender's network, and should not include offensive cyber measures in which the confidentiality, integrity, and availability triad is compromised without authorization. When considering incremental improvements from today's cyber security environment, a logical first step is to provide the advantages of the Department of Homeland Security's Continuous Diagnosis and Mitigation program to private industry. Further, private industry's use and contribution to cyber vulnerability and threat information sharing is critical; barriers to participation in the Automated Indicator Sharing program should be aggressively removed, whether through incentives, regulatory control, or mitigation of civil liability. Finally, organizations should develop an investment strategy in building sensor networks that support business operations. This encompasses evaluation and iteration of data useful for collection. Likewise, they should invest in development and maturation of computational models that capture business functions. Rather than trying to model entire systems, such development should be incremental, focusing on the most critical business processes, data sets, or network segments. This, in turn, will feed into improvements in automation.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Scott Jasper, U.S. Navy Captain (retired) of the National Security Affairs Department at the Naval Postgraduate School, and Doctor Ted Lewis, of Creek Technology Inc., and professor (retired) at the Naval Postgraduate School. Both Captain Jasper and Doctor Lewis challenged my thinking and direction of research, and their constructive guidance and encouragement kept me moving forward. They were always there for feedback as I needed it.

I would also like to express my profound gratitude to my wife and son for their unwavering support over the past two years as I pursued my education at the Naval Postgraduate School, to include the writing of this thesis. My completion of the program would not have been possible without them. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This thesis examines if automated cyber defense promises to be more effective than current models to cope with vulnerabilities introduced by the projected increase in internet-enabled devices. The question is scoped to foresee cyberspace landscape evolution over the next 10 to 15 years. In particular, the author claims the anticipated exponential growth of Internet of Things (IoT) devices will open vulnerabilities at such a rate that current manual methods of detection, verification, and remediation will not be able to keep up. The thesis then explains why the automation of cyber defenses is more effective than current models in performing methodical tasks, and why such automation will be required to handle the oncoming crush of IoT devices and associated vulnerabilities. Anticipated technological developments critical to automation are examined, which organizations should be able to leverage to enhance their cybersecurity posture.

Current defensive models and efforts are not adequate to defend networks from the volume of vulnerabilities introduced through IoT devices. Three gaps contribute to this: 1) the expected exponential growth of IoT devices, 2) limited growth of IT security personnel and budgets, and 3) an increase in cyber attacks, to include machine-to-machine attacks.

Three core technological components are identified as essential toward realizing the automated defenses of cyber systems (ADCS): sensors, autonomic computing, and artificial intelligence (AI). Various technological advancements are cited as evidence of each component's emergence. The realization of ADCS will likely arrive piecemeal, with incremental improvements to the sensor, autonomic, and AI components. The purpose of this thesis is to inform policy on acceptance of the ADCS model, and to encourage accelerated research and investment into the aforementioned components.

A. BACKGROUND

Despite periodic embarrassing revelations of cyber attacks, today's organizations do their best to internally manage cybersecurity risks through various mitigation strategies. Impacted consumers typically recognize their involvement only when they are notified, usually with an offer of free credit monitoring or a new credit card. However, this will change as consumers increasingly use IoT devices in almost every imaginable way. A glimpse of what is to come was recently shown when Fisher-Price acknowledged a vulnerability in one of its WiFi-connected smart toy bear lines that had the potential to expose children's personally identifiable information (PII).[1]

The mass proliferation of internet-enabled devices has the potential to unravel traditional cyber attack coping mechanisms. The Federal Bureau of Investigation (FBI) has warned of threats associated with the spread of IoT devices, stating it "increases the target space for malicious actors."[2] Typical IoT devices are smartphones, closed-circuit television (CCTV) cameras, connected cars, industrial sensors connected to the internet, and emerging smart devices such as smart watches and appliances. In the near-term future, IoT will encompass any product of any size that communicates through the internet.

Left unchecked, risk managers in government and the private sector will struggle to secure burgeoning attack surfaces, and impacts from successful cyber attacks are likely to increase in frequency and severity. An attack surface of a software environment is "the sum of the different points (the 'attack vectors') where an unauthorized user (the 'attacker') can try to enter data to or extract data from an environment."[3]

[1] "Researchers Discover a Not-So-Smart Flaw in Smart Toy Bear," Trend Micro, February 4, 2016, http://www.trendmicro.com/vinfo/us/security/news/Internet-of-things/researchers-discover-flaw-in-smart-toy-bear.

[2] Douglas Bonderud, "IoT Warning: FBI Says More Devices Equal Bigger Attack Surface," *Security Intelligence*, last modified September 15, 2015, https://securityintelligence.com/news/iot-warning-fbi-says-more-devices-equal-bigger-attack-surface/.

[3] *Wikipedia*, s.v. "Attack Surface," last modified September 8, 2015, https://en.wikipedia.org/wiki/Attack_surface.

A recent example was revealed in June 2016 when the cybersecurity firm Securi reported a distributed denial of service attack targeting a small business. What made this attack relevant is that the underlying botnet[4] was attributed to over 25,000 compromised internet-enabled CCTVs, devices that most consumers do not think of as networked computers. Furthermore, the devices were spread out globally and came from various CCTV vendors.[5] This suggested the devices were compromised by a single exploit, possibly through a previously disclosed vulnerability in digital video recording software commonly used within CCTV devices to allow remote code execution.[6] In lay terms, the bad guy—who may have been across the street or on another continent—executed programs on another person's computer without the owner's knowledge or consent. This was not only bad for the small business targeted by the botnet, but also for every one of the CCTV owners who gave a skilled hacker an entryway into their corporate, business, or home networks.

Current cybersecurity models were developed in a pre-IoT internet era, most frequently characterized by a client/server environment in which desktop and laptop computers were clients, and rack-mounted hardware were servers. Unfortunately, these models are insufficient to address vulnerabilities associated with the impending expansion of cyber surface area through IoT. Furthermore, the number of cybersecurity professionals will not grow at the same rate as the devices requiring protection. This will result in expanding gaps in cyber defenses. The compromise of vulnerable devices connected to the internet will foster malicious actor attempts to disrupt or gain access to all types of sensitive networks. Consequences will magnify as governments, businesses, and individuals grow increasingly dependent on these networks.

[4] From *Wikipedia*, "A botnet is a number of Internet-connected computers communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control (C&C) or by passing messages to one another (C&C might be built into the botnet as peer-to-peer)." *Wikipedia*, s.v. "Botnet," last modified September 1, 2016, https://en.wikipedia.org/wiki/Botnet.

[5] Daniel Cid, "Large CCTV Botnet Leveraged in DDos Attacks," *sucuri*, last modified June 27, 2016, https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html.

[6] Rotem Kerner, "Remote Code Execution in CCTV-DVR Affecting over 70 Different Vendors," *Kerner on Security*, March 22, 2016, http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html.

While eliminating all cyber risk is not reasonable, a better choice over today's cybersecurity models is needed that will allow cybersecurity professionals to manage vulnerabilities on more complex networks with exponentially more devices. This thesis proposes such a model.

B. METHODOLOGY

The research is based upon a review of cybersecurity literature, which includes academic books, peer-reviewed articles, research papers, government publications, testimony before Congress, commercial literature, news articles, and online blogs conversant with the topic. As an exploratory effort, relevant points of information were extracted and presented to build a logical narrative describing the current and predictive future state of cyber attacks and available cybersecurity solutions.

C. OVERVIEW

Chapter II describes impending threats in terms of trends in internet-based technologies that will shape the future cyberspace landscape. The vulnerabilities come primarily from IoT and how quickly these devices will be deployed, trends in IT security personnel and budget investments, and the motivations of malicious actors. Changes around the cost structure and frequency of cyber attacks are also reviewed.

Chapter III examines current cybersecurity models, starting with significant historical roots of the security challenges we face today and will face in the future. Four prominent cybersecurity models are presented: 1) network boundary control, 2) defense-in-depth, 3) continuous monitoring, and 4) intelligence driven. Finally, four recent and critical cybersecurity initiatives, designed to address current threats are reviewed: 1) the National Institute of Standards and Technology (NIST) Cybersecurity Framework, 2) Automated Indicator Sharing (AIS), 3) Continuous Diagnosis and Monitoring (CDM), and 4) Active Cyber Defense (ACD).

Chapter IV proposes a change in cybersecurity approach called automated defense of cyber systems (ADCS). It represents two critical shifts in cyber defense: a move away from current client/server conceptual models to a much more complex, organic perspective of networked systems; and an evolution from manual, human-driven interventions to automation. Three core technological components are critical toward realizing this evolution, which are 1) mass promulgation of internet-enabled sensors, 2) autonomic computing, and 3) artificial intelligence techniques.

Chapter V provides findings, conclusions, and recommendations, which are geared to both cybersecurity professionals and policy makers, and designed to accelerate adoption of ADCS. The chapter also suggests several areas of future research for those wishing to continue examining this topic.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FUTURE LANDSCAPE OF CYBERSECURITY

This chapter describes the most likely near-future threats due to the IoT, investment trends for IT security personnel and budgets, and the motivations of three groups of malicious actors. Changes around the cost structure of vulnerabilities, attacks, and defenses are also reviewed.

A. INTERNET OF THINGS IMPACT ON CYBERSPACE

The IoT is defined as "interrelated computing devices, mechanical and digital machines, objects, [etc.] with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."[7] Such devices include not just smartphones and tablets, but wearable health monitors, televisions that stream videos, and sensors that read voltage on power lines, to name only a few.

In 2015, nearly two-thirds of American adults had a smartphone, 90 percent had broadband service at home, and only 7 percent had neither a smartphone nor broadband service at home.[8] In January 2015, there were over 50 million publically available WiFi hotspots globally, and the number is projected to reach 340 million by 2018.[9] With this infrastructure in place, an overwhelming majority of Americans have ready access to highly functional devices connected to the internet, which will act as gateways to take advantage of IoT devices and capabilities. Citizens will be able to access their IoT devices from virtually anywhere. We will increasingly work, learn, socialize, pay our bills, lock our doors, monitor our heart rate, watch our children or favorite zoo animals, and check the contents of our refrigerator, all from anywhere with a signal.

[7] Margaret Rouse, "Internet of Things (IoT)," Whatis.com, accessed August 28, 2016, http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[8] Aaron Smith, "U.S. Smartphone Use in 2015," Pew Research Center, April 1, 2015, 2–3, http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

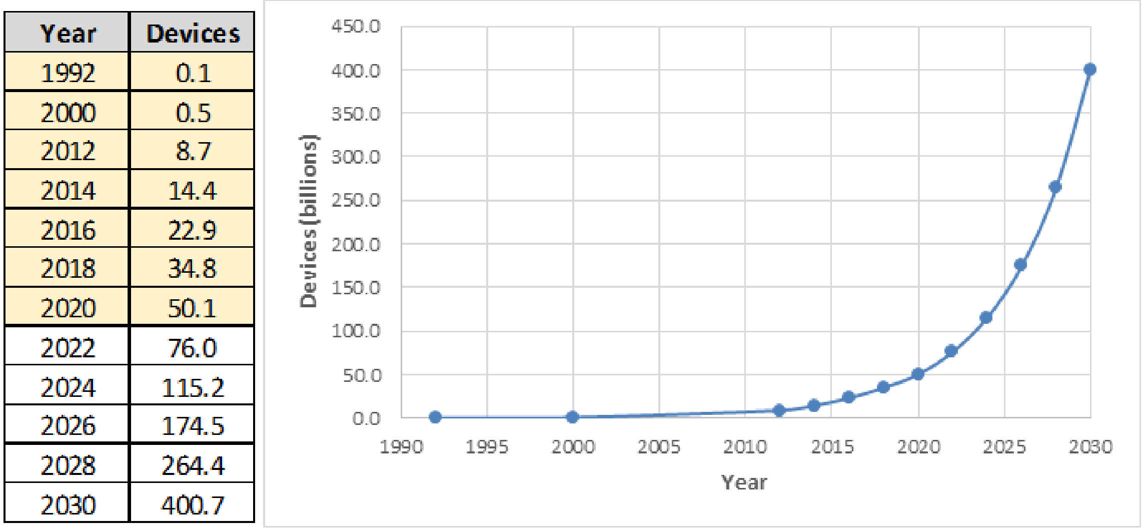
[9] "The Global Public Wi-Fi Network Grows to 50 Million Worldwide Wi-Fi Hotspots," IPass, January 20, 2015, https://www.ipass.com/press-releases/the-global-public-wi-fi-network-grows-to-50-million-worldwide-wi-fi-hotspots/.

1. Exponential Growth

Within the next decade, IoT devices will dominate the cyber landscape. In a research brief published in September 2015, CompTIA projected compound growth of 23.1 percent annually, with over 50.1 million devices by 2020.[10] Using CompTIA's historic and projected data points, a calculation of growth can be expressed by the following formula:

Number of Devices in Billions = 0.121 * 1.231^(Year – 1991).

As illustrated in Figure 1, this calculates out to an astounding 400+ billion devices by 2030. While the value of the coefficient in this formula is up for debate, such projections are entirely plausible given potential reduction in cost, size, and power requirements for each IoT device, along with increases in business application and efficiencies as commercial IoT solutions emerge. The critical concept is that deployment is on an exponential growth curve, and that we are only at the beginning of that curve.



Year	Devices
1992	0.1
2000	0.5
2012	8.7
2014	14.4
2016	22.9
2018	34.8
2020	50.1
2022	76.0
2024	115.2
2026	174.5
2028	264.4
2030	400.7

Figure 1. Projected Number of IoT Devices

[10] CompTIA, "Sizing up the Internet of Things," August 28, 2015, 4, https://www.comptia.org/resources/sizing-up-the-internet-of-things.

Improvement—and subsequent adoption—of a new technology is frequently described in terms of an S-curve. Harvard business professor Clayton Christensen explains an S-curve as slow progress in early stages, increasing as the technology becomes better understood and slowing as it approaches a natural or physical limit.[11] Figure 1 only shows the beginning of the S-curve, and it is reasonable to question when IoT market saturation will occur. However, market saturation is unlikely to occur for IoT device integration, at least during the projected period; advances in computational capacity and miniaturization will propel new and innovative uses of IoT devices. According to Professor Jianguo Ding, University of Skövde, "Computing is deeply embedded into every physical component, possibly even into materials."[12] Unlike traditional markets, where physical limits are often associated with the number of people (e.g., the percentage of device ownership approaches 100 percent), there does not appear to be a limit of IoT devices per person. As is later argued in Chapter IV, traditional networks of servers and wires will almost completely cease to exist, replaced by mobile nanodevices, which are tiny computers measured in nanometers with integrated wireless connectivity. Therefore, maturation in the IoT S-curve cannot be reasonably projected until a better understanding of the natural and physical limits are understood.

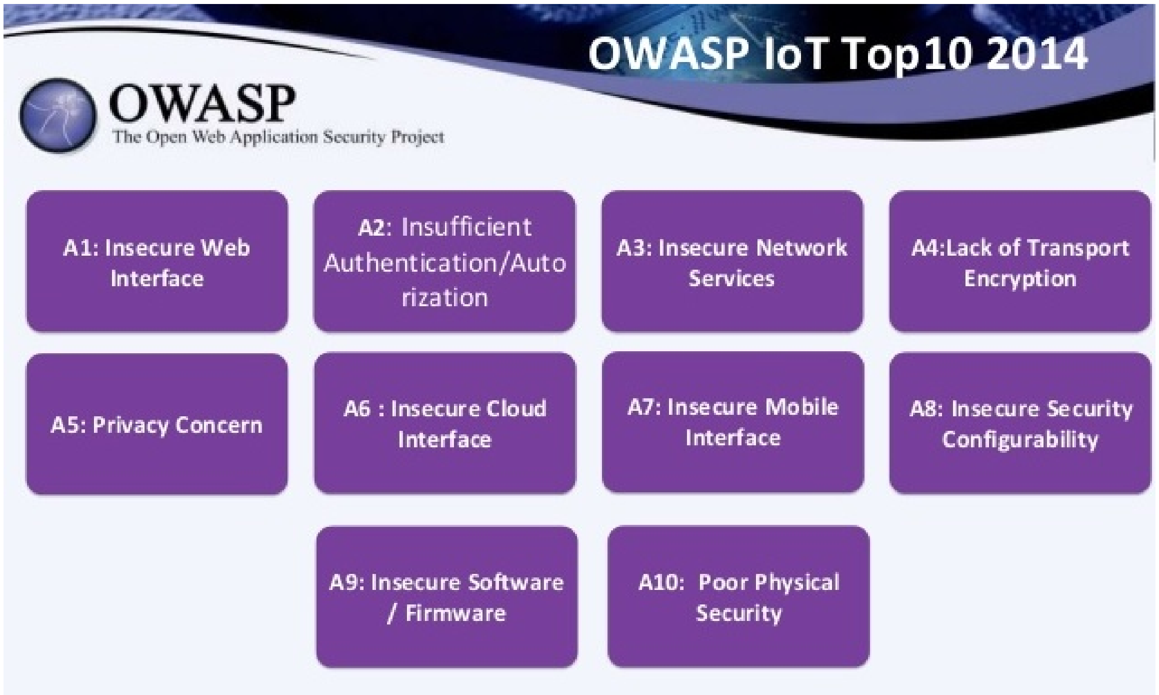
2. IoT Impact on Cybersecurity

The IoT is vastly expanding the attack surface vulnerable to malicious exploitation. To more precisely specify what is included within the IoT attack surface, the not-for-profit Open Web Application Security Project (OWASP) drafted a mapping of 19 distinct IoT attack surface area categories to 130 vulnerability types, and then published the list of top ten vulnerabilities (see Figure 2). These findings were more recently supported by Hewlett Packard Enterprise in 2015. Hewlett Packard's study of common household IoT devices found that 80 percent used weak passwords (susceptible to brute force password attacks), 70 percent used unencrypted services (susceptible to network

[11] Clayton M. Christensen, "Exploring the Limits of the Technology S-curve. Part I: Component Technologies," *Production and Operations Management* 1, no. 4 (Fall 1992): 334.

[12] Jianguo Ding, "Intrusion Detection, Prevention, and Response System (IDPRS) for Cyber-Physical Systems (CPSs)," in *Securing Cyber-Physical* Systems, ed. Al-Sakib Khan Pathan (Boca Raton, FL: CRC Press, 2015), 373.

sniffing), 70% allowed account enumeration (allows refined attack targeting), and 60% exhibited user interface vulnerabilities (persistent cross-site scripting and weak credentials).[13] To demonstrate growth in potential exploitation of these vulnerabilities, a 2016 AT&T Security Operations Center report noted a 458 percent increase in IoT vulnerability scans over the past two years.[14]



OWASP IoT Top10 2014

OWASP
The Open Web Application Security Project

A1: Insecure Web Interface

A2: Insufficient Authentication/Autorization

A3: Insecure Network Services

A4:Lack of Transport Encryption

A5: Privacy Concern

A6 : Insecure Cloud Interface

A7: Insecure Mobile Interface

A8: Insecure Security Configurability

A9: Insecure Software / Firmware

A10: Poor Physical Security

Figure 2. OWASP Top10 IoT Vulnerabilities in 2014[15]

Even skeptics among cybersecurity professionals acknowledge the eventual emergence of risk associated with the IoT. Andrzej Kawalec, head of security research and chief technology officer at Hewlett Packer Security Services, stated, "Although there may be an immediate threat to business due to some consumer IoT device that's been

[13] "Internet of Things Research Study," Hewlett Packard Enterprise, November 2015, 4, https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[14] "The CEO's Guide to Security the Internet of Things," AT&T, 2016, 8, https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf.

[15] Source: Sebastien Gioria, "CLUSIRInfoNord OWASP IoT 2014," LinkedIn, January 20, 2015, http://www.slideshare.net/SebastienGioria/clusir-infonord-owasp-iot-2014.

adopted, most businesses will only face this in around five years' time."[16] Despite downplaying current risk, his full statement made clear that specific early-adopter industries (e.g., healthcare, hotels) are currently vulnerable, and that it is only a matter of time before competitive advantage forces industries to adopt IoT devices. Kawalec described this moment as the "IoT tsunami."

B. IT SECURITY PERSONNEL AND BUDGETS

1. IT Security Personnel

While the number of managed devices grows exponentially, the number of personnel responsible for securing those devices will not. According to the Bureau of Labor Statistics (BLS), the job growth outlook for information security analysts is 18 percent between 2014 and 2024, starting in 2014 at 82,900 positions.[17] BLS projects an 8-percent growth rate for network and computer systems administrators—a position that overlaps significantly with information security analysts—over the same period, starting with 382,600 positions. Combined, they project an average growth rate of 9.8 percent, with a 2014 base of 465,500 positions.[18]

While the combined growth figure for these two positions is higher than the BLS average job growth outlook of 7 percent, it is negligible compared to the projected 800 percent growth of IoT devices during the same timeframe. If position productivity were measured by an employee's ability to manage a set number of devices, and presuming the U.S. growth of IoT devices mirrors the global projection provided in Section A1, the 2024 employee would have to manage 730 percent more devices than his or her 2014 counterpart.

[16] Warwick Ashford, "Exploding IoT attack surface Not an Immediate Threat to Business," ComputerWeekly, May 27, 2016, http://www.computerweekly.com/news/450297327/Exploding-IoT-attack-surface-not-an-immediate-threat-to-business.

[17] "Occupational Outlook Handbook: Information Security Analyst," Department of Labor Bureau of Labor Statistics, December 17, 2015, http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[18] "Occupational Outlook Handbook: Network and Computer Systems Administrators," Department of Labor Bureau of Labor Statistics, December 17, 2015, http://www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm.

2. IT Security Budgets

The investment in IT security budgets, which is anticipated to grow, also pales in comparison to the 23.1 percent compound growth of IoT devices. Gartner, Inc. assessed global IT spending at $75.4 billion in 2015, and projects the market will grow at compound annual growth rate of 7.8 percent through 2019, which equates to annual spending north of $100 billion at that time.[19] Overall IT spending is expected to grow only 1.9 percent.

As Mark Lobel of PricewaterhouseCoopers (PwC) put it, “Strategic security spending demands that businesses … fund processes that fully integrate predictive, preventive, detective, and incidence response capabilities.”[20] However, given the anticipated personnel increase, a significant portion of the IT spending growth can reasonably be expected to pay for salaries, to include salary growth from inflation. Only a portion of those funds, whether funded through IT security budgets or general IT budgets, will be available for investment in employee productivity.

C. MALICIOUS ACTORS

This section assesses if categories of cyber actors unacceptably disrupting social order today will continue to do so in the future. Understanding motivations, and how they may evolve, is an important component in understanding the threat environment within which a defender exists. The FBI has identified three broad groups that constitute cyber threats today: terrorists, state-sponsored actors, and criminal organizations.[21] Given history and human nature, it is fair to assume these threats will persist.

[19] “Gartner says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach 75.4 Billion in 2015,” Gartner, September 23, 2015, http://www.gartner.com/newsroom/id/3135617; “Forecast Analysis: Information Security, Wordwide, 4Q15 Update,” Gartner, March 22, 2016, https://www.gartner.com/doc/3261517/forecast-analysis-information-security-worldwide.

[20] “Security Incidents Continue to Rise in Cost and Frequency while Budgets Decrease, According to PwC, CIO and SCO’s The Global State of Information Security Survey 2015,” PricewaterhouseCoopers, September 30, 2014, http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html.

[21] Shawn Henry, “Cyber Threat: On the Front Lines with Shawn Henry,” Federal Bureau of Investigation, March 27, 2012, https://ucr.fbi.gov/news/stories/2012/march/shawn-henry_032712/shawn-henry_032712.

1. Terrorism

Terrorism, in the traditional sense of the term, is defined within the United States by 18 U.S.C. § 2331. While the statute differentiates between domestic and international terrorism, both comprise a violent or dangerous act that violates U.S. law with the intent "(a) to intimidate or coerce a civilian population; (b) to influence the policy of a government by intimidation or coercion; or (c) to affect the conduct of a government by mass destruction, assassination, or kidnapping." The difference between domestic and international terrorism is, as the words imply, whether the perpetrator's desired effect occurs primarily inside or outside the territorial jurisdiction of the United States.[22] The term "cyber terrorism," in comparison, does not have a formal legal definition. It often conflates issues such as unauthorized hacking, propaganda dissemination, and recruitment.[23] To limit scope, Jian Hua and Sanjay Bapna proposed that cyber terrorism is an act performed by individuals who seek to deny the confidentiality, integrity, or availability of networked computing technologies, to include data, from authorized users, for the purpose of either interfering with significant political, social, or economic functioning, or to induce physical violence or panic.[24]

Terrorist organizations are increasingly using cyber terrorism, as Hua and Bapna defined it, to meet their objectives. While analyzing news media coverage of cyber terrorism matters, researchers identified an increase in related articles, calculating an average of 2.2 items per month for the 33 months prior to 2010, and 5.4 per month in the following 32 months—an increase of 236 percent.[25] In explaining cyberterrorism's strategic advantages for potential attackers, John Klein of Falcon Research cited very low start-up costs, enhanced anonymity over kinetic methods, a wide swath of potential

[22] *Crimes and Criminal Procedure*, 18 U.S.C. § 2331.

[23] E. E. Nesmeyanov, A. M. Rudenko, and V. V. Kotlyarova, "Sociocultural Analysis of Cyberterrorism in Social Nets within the Problems of Information Safety of Russian Society," *Science Almanaca Black Sea Countries* 4 (2015): 3.

[24] Jian Hua and Sanjay Bapna, "The Economic Impact of Cyber Terrorism," *The Journal of Strategic Information Systems* 22, no. 2 (2013): 3.

[25] Lee Jarvis, Stuart Macdonald, and Andrew Whiting, "Constructing Cyberterrorism as a Security Threat: A Study of International News Media Coverage," *Perspectives on Terrorism* 9, no. 1 (2015).

targets, and the ability to conduct attacks remotely.[26] Examples of cyber attacks include: a) intimidating a target, often through denial-of-service attacks in which ongoing business operations supported through networked technology are disrupted; b) delivering propaganda by co-opting and defacing networked information delivery mechanisms; and c) obtaining and releasing information to facilitate kinetic targeting of specific locations or individuals.

Future terrorists will see cyberterrorism as a quick and cost-effective means to move their agendas forward. Additionally, as technology becomes further integrated and available worldwide, potential cyber terrorists will have both an entry point from which to conduct a cyber attack and a better understanding of society's reliance on internet-based technologies.

2. Nation States

When providing the "Worldwide Threat Assessment of the U.S. Intelligence Community" to the Senate Armed Services Committee, the director of national intelligence led with cyber and technology threats from other nation states.[27] When considering cyber attackers, the term "state-sponsored" refers to the disruption or obtainment of unauthorized access to networked systems by countries, or their proxies, to achieve a national objective. Nations have broad ranges of military, political, and economic interests, and state-sponsored hacking is inclusive of both cyberwarfare—characterized by attacks intended to damage or deny advantage at the strategic, tactical, and operational levels—and cyber espionage—characterized by clandestine intelligence collection and covert operations conducted predominantly online.[28] Given the availability of networked systems impacting those interests, the number of potential targets is limited

[26] John J. Klein, "Deterring and Dissuading Cyberterrorism," *Journal of Strategic Security* 8, no. 4 (2015): 27–28.

[27] *Testimony before the U.S. Senate Armed Services Committee* (2016) ("Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," James R. Clapper), 2–4, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

[28] Maren Leed, *Offensive Cyber Capabilities at the Operational Level*, (Washington, DC: Center for Strategic International Studies, 2013), 2, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf.

by only two factors: 1) a nation’s laws and policies on acceptable norms of behavior in cyberspace, and 2) resources available to pursue targets.

While sensitive techniques associated with military action are often classified, instances of alleged cyberwarfare have been documented, likely due to their directly observable impacts. One of the earliest examples involved the targeting of U.S. computers by the Yugoslav air defense system during the 1998 conflict.[29] In another example, cyber attackers were alleged to be directed, or intentionally incited, by the Russian government in response to a 2007 political incident; these cyber attacks effectively disrupted internet-based services in Estonia, thereby contributing to regional chaos in a manner that Russia could exploit.[30] Similarly, Islamic Revolutionary Guard Corps–led Iranian hackers allegedly conducted a series of denial-of-service attacks in 2012 against a large number of U.S. financial sector institutions,[31] presumably “in response to increasingly strong economic sanctions imposed by the United States and Europe in an attempt to force Iran to curtail its nuclear program.”[32]

State-sponsored cyber espionage, by nature, is hidden by perpetrators via state secrets. Unlike cyberwarfare, well-executed cyber espionage attacks are not directly observable, and concrete examples are hard to find. The range of cyber espionage activities include recruiting human intelligence, spying on dissident expatriate communities, gaining economic advantage or foreign influence, and obtaining foreign government information. The People’s Republic of China’s (PRC) global targeting of proprietary and commercial information, for example, is well documented in reports by various governments, and has fueled a massive expansion of private cybersecurity firms. These firms have produced detailed technical reports that suggest the PRC is transitioning

[29] Bradley Graham, “Military Grappling with Rules for Cyber Warfare,” *Washington Post*, November 8, 1999, http://www.washingtonpost.com.

[30] Jason Richards “Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security,” *International Affairs Review* 18, no. 2 (2009).

[31] “International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector,” Federal Bureau of Investigation, March 24, 2016, https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector.

[32] Ellen Nakashima and Matt Zapotosky, “U.S. Charges Iran-Linked Hackers with Targeting Banks, N.Y, Dam,” *Washington Post*, March 24, 2016, https://www.washingtonpost.com.

from seeking volume to pursuing focused cyber attack targeting.[33] In its 2015 Global Threat Report, Crowdstrike opined the PRC's massive targeting of PII across various public and private databases could enable identification of individuals with access and potentially susceptible to recruitment.[34] Additionally, the Russian government is suspected of leaking Democratic National Committee emails to WikiLeaks during the 2016 U.S. presidential election cycle, possibly to create domestic turmoil and to move the United States to a less-engaged position globally.[35]

These examples show that valuable targets are available to sovereign entities, with promise for relatively quick and inexpensive national gain when compared to diplomacy, public policy, or judicial processes. Considering the expanded network surface via the IoT, nation states will have exponentially greater avenues through which to exploit targets. Senior Defense Analyst Brian Mazanec captured it best when he wrote, "The norm evolution theory for emerging-technology weapons predicts grim prospects for the evolution of constraining cyber norms."[36]

3. Organized Crime

Organized crime, and its corresponding definition, has changed as a result of law enforcement's targeted disruption efforts. Forty years ago, organized crime was predominantly seen as monolithic, often limited by ethnicity and motivated by greed and territorial power. A contemporary view of organized crime is far more inclusive of loosely coupled networks of groups and individuals with varying motivations. These can include traditional criminal goals of monetary gain, but also "intellectual challenge, individual or group notoriety, lust …, ideology, rebellion, and curiosity."[37] Such groups

[33] "Redline Drawn: China Recalculates its Use of Cyber Espionage," FireEye, accessed August 21, 2016, 15, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

[34] "2015 Crowdstrike Global Threat Report," Crowdstrike, accessed August 21, 2016, 6, https://www.crowdstrike.com/global-threat-report-2015/.

[35] David E. Sanger and Eric Schmitt, "Spy Agency Consensus Grows That Russia Hacked D.N.C.," *New York Times*, July 26, 2016, http://www.nytimes.com.

[36] Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable," *Strategic Studies Quarterly* 9, no. 2 (2015): 95.

[37] Roderic Broadhurst et al., "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime," *International Journal of Cyber Criminology* 8, no. 1 (2014): 3.

lend themselves well to the internet's distributed and often anonymous nature. In characterizing the transition from offline to online groups conducting cybercrime, criminologist Dr. Michael McGuire modeled six types of group structures: swarm, hub, clustered hybrid, extended hybrid, hierarchy, and aggregate groups.[38] The first two operate predominantly online, the third and fourth mix online and offline activity, and the fifth and sixth are predominantly offline. The online elements of the first four groups are often fluid, requiring technical and expert ebb and flow to meet a specific criminal goal.[39]

In addition to adapting their structure, criminals adapt their techniques to evade law enforcement. Using open source and commercially available tools allow criminals to obscure both the origin and contents of internet communication. The evolution of ransomware between Cryptolocker and CryptoWall demonstrated the integration of the Onion Router (to obfuscate network traffic patterns) and virtual currency payment (to avoid financial transaction reporting).[40] Another such adaptation is criminal use of encryption and ephemeral services to hinder law enforcement's ability to search or intercept communications, which has been outlined by the FBI in a phenomenon called "Going Dark."[41]

D. INCENTIVES AND FREQUENCY OF CYBER ATTACKS

An examination of attacker and defender incentives shows resource costs decreasing for attackers, while increasing for defenders. This will likely elevate cyber attacks, as actors frequently possess both the resources and intent to conduct an attack. Furthermore, the frequency of attacks is increasing.

[38] Ibid.

[39] Broadhurst et al., "Organizations and Cyber Crime," 3.

[40] *Oversight of the Federal Bureau of Investigation* (December 9, 2015) (testimony of James B. Comey before the U.S. Senate Judiciary Committee), https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-8.

[41] "Going Dark," Federal Bureau of Investigation, accessed July 29, 2016, https://www.fbi.gov/services/operational-technology/going-dark.

1. Cost to Attack

The cost to build and use cyber tools to exploit cyber vulnerabilities is low and decreasing. Hacking toolkits are frequently updated and readily available. Many are free, openly developed, and co-opted from legitimate network security uses (e.g., nmap, cain & able, and Nikto).[42] The price of a remote access Trojan went from between $50 and $250 in 2013 to between $5 and $10 in 2016.[43] Distributed denial-of-service attacks were sold for $50 per night.[44] Particularly disturbing research from Dell SecureWorks in 2016 showed that some of these markets have been allowed to mature in relative stability, to a point where they have incorporated higher-functioning business processes built around customer service and guarantees of value.[45]

The cost to obtain criminal means that enable cyber attacks is also decreasing, evident in analysis of virtual black markets between 2005 and 2011. The analysis indicated that standard U.S. credit cards were sold for $6 and skimmers, used to steal credit card data, ranged from $425 to $6,000.[46] Dell Secureworks further showed that virtual marketplaces are flooded with counterfeit documents, and that the breadth and depth of stolen financial information has expanded. Between 2014 and 2016, the cost of a matching social security card, driver's license, and utility bill dropped from $350 to $90.[47]

Beyond criminal use, the cost of state-sponsored advanced malware has dropped precipitously. Costin Raiu, head of global research and analysis at Kaspersky Lab, stated during a prepared speech that Stuxnet, an early cyber weapon that targeted Iran's nuclear

[42] "Hacker Tools Top Ten: Our Recommended Tools for 2016," Concise AC, accessed August 26, 2016, https://www.concise-courses.com/hacking-tools/top-ten/.

[43] Ibid., 4.

[44] Ziming Zhao et al., "Mules, Seals, and Attacking Tools: Analyzing 12 Online Marketplaces," *IEEE Security & Privacy* 14, no. 3 (2016): 37.

[45] "Underground Hacker Markets," Dell SecureWorks, 2016, 7, https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report.

[46] Zhao et al. "Mules, Seals, and Attacking Tools," 37.

[47] "Underground Hacker Markets," Dell SecureWorks, 5, 14.

development program, was estimated to cost $100 million.[48] The IceFog malware, which targeted U.S. energy companies, was hypothesized to cost $10,000. Raiu went on to opine, "The cost of entry for [advanced persistent threats] is decreasing …. We're going to see more surgical strikes and critical infrastructure attacks."[49]

2. Cost of an Attack

The cost borne by cyber attack victims is increasing. A 2014 report by Intel Security (McAfee) estimated the damage caused by cybercrime to be more than $400 billion annually.[50] Analysis conducted by Juniper Research projects cyber data breaches will globally cost society $2.1 trillion by 2019—a fourfold increase over their estimated breach costs for 2015, compounding at an astonishing annual rate of 41 percent.[51] HP Enterprise Security underwrote a 2015 survey of 252 large organizations (1000+ individuals) on the global cost caused by cybercrime, cataloging 1,928 total attacks, and found that the mean cost associated with an incident was $7.7 million.[52] The study has been repeated annually with incident costs on the rise, albeit at an annual rate of 1.9 percent. Of the external costs incurred, the top three impacted areas were business disruption (39 percent), information loss (35 percent), and revenue loss (21 percent).[53]

3. Attack Frequency

In testimony before the U.S. House of Representatives, FBI Assistant Director Joseph Demarest stated, "The frequency and impact of cyber attacks on our nation's private sector and government networks have increased dramatically in the past decade

[48] Pierluigi Paganini, "Speaking at Kaspersky Lab's Industry Analyst Summit Costin Raiu, Revealed that the Cost for APT Campaign is Dramatically Dropping," *Security Affairs*, February 9, 2014, http://securityaffairs.co/wordpress/22056/cyber-crime/apt-cost-dramatically-dropping.html.

[49] Ibid.

[50] Intel Security, *Net Losses: Estimating the Global Cost of Cybercrime* (Santa Clara, CA: Intel Security Center for Strategic and International Studies 2014), 2.

[51] "Cybercrime Will Cost Businesses Over $2 Trillion by 2019," Juniper Research, May 12, 2015, http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

[52] Ponemon Institute, *2015 Global Report on the Cost of Cyber Crime* (Traverse City, ME: Ponemon Institute, 2015), 6.

[53] Ibid., 16.

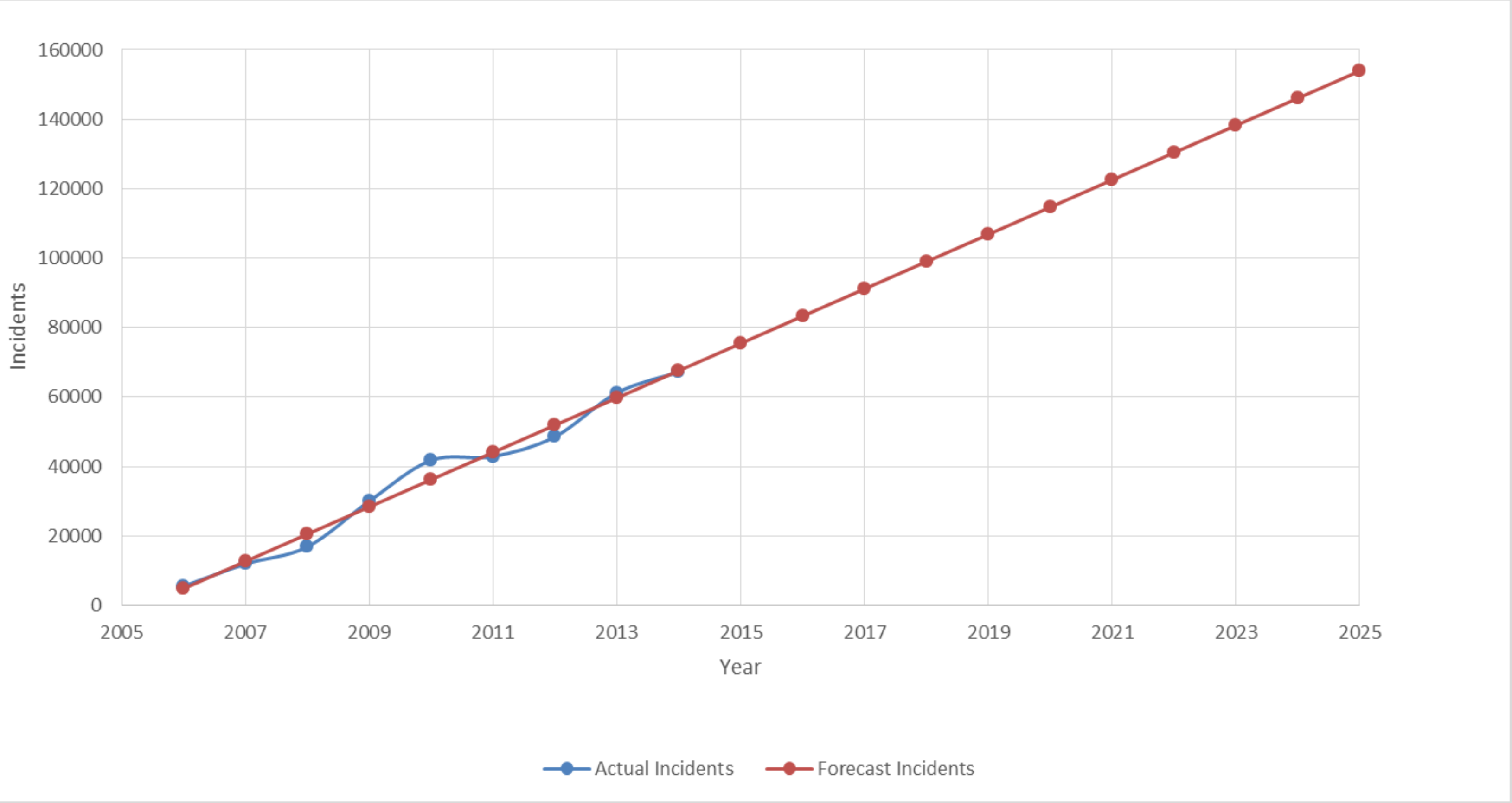
and are expected to continue to grow."[54] A PwC survey showed 42.8 million security incidents in 2015, with the data indicating that the compound annual growth rate of detected security incidents "has increased 66 percent year over year since 2009."[55]

The number of cybersecurity incidents continues to rise. During testimony for the U.S. House of Representatives, Government Accountability Office Director Gregory C. Wilshusen presented a chart demonstrating growth in cyber incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team, growing from 5,503 in 2006 to 67,168 in 2014.[56] The data suggest a linear growth rate (see Figure 3), which projects over 150,000 reported incidents on federal systems by 2025.

[54] Joseph Demarest, "Statement of Joseph Demarest Assistant Director Cyber Division Federal Bureau of Investigation," *Testimony before the U.S. House of Representatives Homeland Security Committee*, May 21, 2014, 2.

[55] "Security Incidents Continue to Rise," PricewaterhouseCoopers.

[56] *Information Security, Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies* (July 18, 2015) (Testimony of Gregory C. Wilshusen, before the U.S. House of Representatives, Subcommittee on Research and Technology and Oversight), 7, http://www.gao.gov/assets/680/671253.pdf.



Actual incidents were adapted from data in Wilshusen, "Information Security." Forecast incidents were projected consistent with actual incident data.

Figure 3. Projecting Federal Cyber Incidents Reported to US-CERT

Machine-to-machine attacks may push the number of cyber attacks to a growth curve similar to the integration of IoT devices. Cybersecurity experts have predicted 2016 will see the first generation of worms and viruses targeting “headless devices,” which are IoT devices without user interfaces that are controlled by hub devices, such as a smartphone.[57]

In their examination of botnet designed to send spam email, Proofpoint observed that “25 percent of the volume was sent by … everyday consumer gadgets such as compromised home networking routers, connected multi-media centers, televisions and at least one refrigerator.”[58] Two viable vectors of malicious code introduction include through the hub device (e.g., a smartphone downloads a compromised app) and supply chain (i.e., a new product ships with embedded malicious software).

To summarize, the incentives for attackers are increasing, the impact to victims is increasing, and the frequency of attacks is increasing. While a causal relationship between the three is not explicitly drawn, the correlation is apparent. Attack costs and frequency remain valid metrics through which to evaluate the efficacy of future cybersecurity efforts.

[57] Harriet Taylor, “Biggest Cybersecurity Threats in 2016,” CNBC, December 28, 2015, http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html.

[58] Pierluigi Paganini, “Proofpoint Discovered More Than 750,000 Phishing and SPAM Emails Launched from ‘Thingbots’ Including Televisions, Fridge,” *Security Affairs*, January 19, 2014, http://securityaffairs.co/wordpress/21397/cyber-crime/iot-cyberattack-large-scale.html.

III. CURRENT CYBERSECURITY EFFORTS

A. A FEW WORDS ABOUT THE INTERNET

1. Origins of Cybersecurity

Cybersecurity efforts are rooted in three core principles toward protecting data processed by networked computers: confidentiality, integrity, and availability. In brief, confidentiality preserves privacy for and between authorized users of data, integrity ensures the data being processed has not been maliciously or unintentionally altered, and availability means users are able to access and use the data when they want to. These principles are collectively referred to as the "CIA triad," and are the bedrock upon which the security of devices and systems are evaluated.[59] They are applied to data at rest (saved to a hard drive or memory card), in process (being actively manipulated by a computing device), and in motion (being transmitted between devices over a network segment). Any malicious attempt to compromise the CIA triad is a cyber attack, whether successful or not.

An additional cybersecurity concept can be considered as part of the "I" within the CIA triad: non-repudiation, defined as "proof of the integrity and origin of data that can be verified by a third party."[60] Non-repudiation is frequently associated with accountability of digital actions with a specific user, such as through a digital signature. Since 1988, progress toward achieving non-repudiation over the internet has been supported through the X.509 Public Key Infrastructure (PKI), which comprises a set of cryptographic standards implemented in a number of protocols, such as secure web browsing and the exchange of encrypted email.[61] PKI is often associated with authentication—which confirms and ensures a computer user's identity—and

[59] Terry Chia, "Confidentiality, Integrity, Availability: The Three Components of the CIA Triad," *IT Security Community Blog*, August 20, 2012, http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/.

[60] General Accounting Office, *Information Security: Technologies to Secure Federal Systems* (GAO-04-467) (Washington, DC: General Accounting Office, 2004).

[61] *Technopedia*, s.v. "X.509," accessed September 9, 2016, https://www.techopedia.com/definition/4172/x509.

authorization—which bounds access levels and actions available to a user of a computer system.[62]

2. Inherent Insecurity

The internet is inherently insecure, and the cause of the problem can be tracked down to three issues. First, the internet's creators failed to fully contemplate security. Vinton Cerf, one of the original designers of the internet, admitted, "We didn't focus on how you could wreck this system intentionally."[63] To the internet's architects, the dominating security principle was survivability in the event of military action, not the CIA triad. The technologies to build in security were not available or sufficiently mature, in part due to limits in computational power available at the time and export controls on enabling technologies (i.e., encryption).[64] As the designers defined the seven layers of the TCP/IP network stack, the primary objective was reliability. Initial engineering efforts were focused on getting the technology working, not the assurance of the CIA triad. This is why it is often said security was "bolted on" to the internet after the fact.

Second, vulnerabilities are routinely introduced into every layer of the cyber ecosystem, and can never be entirely eliminated. Software bugs are defects in how a program was designed to operate, resulting in software behaviors that were not anticipated by the designer, and hackers seek to exploit bugs to actively circumvent how a program was designed to operate. In a Department of Homeland Security (DHS)-funded analysis, Coverity, Inc. found an error rate of 0.434 defects per thousand lines of code in a broad range of open-source software projects.[65] Each of the TCP/IP layers requires programming, whether implemented in software or hardware. Bugs are fixed

[62] *Technopedia*, s.v. "Authentication," accessed September 9, 2016, https://www.techopedia.com/definition/342/authentication; *Technopedia*, s.v. "Authorization," accessed September 9, 2016, https://www.techopedia.com/definition/10237/authorization.

[63] Craig Timberg, "Net of Insecurity: A Flaw in the Design," *Washington Post*, May 30, 2015, http://www.washingtonpost.com/.

[64] Ibid.

[65] Ben Chelf, *Measuring Software Quality, A Study of Open Source Software* (San Francisco: Coverity, 2006), 3, http://www.coverity.com/library/pdf/open_source_quality_report.pdf.

over time, whether before or after programs are released.[66] However, it is unlikely that programmers will be able to radically reduce future introduction of bugs in new programming efforts. Two factors drive this: the pace of competition to produce and sell new features, and rapid advancement of underlying hardware upon which programs run.

The third fundamental internet security issue is that cyber attacks are a cat-and-mouse game—they are perpetrated and defended by humans, acting and counteracting each other so that one can gain an advantage over the other. Those involved are characterized as "black hats," "white hats," and "gray hats." Black hats work to compromise the CIA triad with malicious intent, while white hats work to ensure the CIA triad, particularly for devices they are charged to protect. Gray hats refer to those who actively work to compromise the CIA triad, perhaps to include conducting activities that have been criminalized, but without malicious intent.[67] Ultimately, the human adversarial dynamic makes it difficult to predict the manifestation of future exploits, which makes it more difficult to defend against them.

B. DEFENSIVE MODELS

Network defenders have designed various models, tools, and techniques to help mitigate a hostile environment in which vulnerabilities are exploited by cyber threats actors. The most prevalent models are presented in this section. These models are not mutually exclusive, and are often used in combination. No model can fully protect a network. The goal of the defender is to reduce risk to an acceptable level at an acceptable cost.

1. Network Boundary Control

The network boundary control model is built upon the assumption that a cyber attack will originate from outside the defended network. Therefore, the simplest mechanism to protect the network would be one that enforces a secure border separating

[66] Steve McConnell, "Software Quality at Top Speed," SteveMcConnel.com, August 1996, http://www.stevemcconnell.com/articles/art04.htm.

[67] Chris Hoffman, "Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats," *How-To Geek*, April 20, 2013, http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/.

the internal network from the external internet. In this model, devices with external network connections are identified, and robust security controls are placed on them. This puts the cybersecurity focus on any and all devices reachable from the internet. The model does not, however, defend devices and services within the network that are not directly accessible from the internet. Such an approach has been described as being like M&M candies, hard on the outside and soft on the inside.[68]

Cybersecurity professionals have largely discounted this approach as a standalone model. A major flaw of this approach is the basic assumption that threats originate from outside an organization. The model is particularly vulnerable to insider threats—those who have authorized access to the defended network but exceed their scope of permissions for an unauthorized purpose. Once a malicious actor breaches the external defenses, the interior network is left unguarded and vulnerable. Another challenge to this model is that modern devices frequently combine plug-and-play configuration with multiple network interfaces, potentially opening holes in the wall unbeknownst to defenders. Despite these flaws, the network boundary control model remains commonly used as a building block within network security architectures to reduce the network surface area directly accessible from the internet.

2. Defense-in-Depth

Defense-in-depth was promulgated to overcome the single point of failure of the network boundary control model, and was conceptualized using the military principle of weakening an adversary by delaying an attacker's advance through the ceding of defended territory. The cyber correlation is to deploy multiple forms of layered defenses, each requiring time and effort for an adversary to defeat, and to give defenders more time to recognize and then mitigate an attack. It provides for information assurance by making

[68] Ted Schlein, "The Five Tough Truths of Cybersecurity," *TechCrunch*, May 31, 2014, https://techcrunch.com/2014/05/31/the-five-tough-truths-of-cybersecurity-software/.

cost-effective security investments focused on people (users), the technology of the system, and the system's operation.[69]

This approach raises the cybersecurity bar by acknowledging malicious events could originate from anywhere, even inside the organization. It also introduced a strategy toward managing security solutions over time, and is considered a best practice by many security professionals.[70] However, the approach has been criticized because historic military advantages from defense-in-depth have not been realized within cyberspace. Specifically, attackers have not been weakened; rather, they are attacking and succeeding at higher rates, and delays from defensive layering have not significantly increased the amount of effort necessary for an attack to succeed.[71]

3. Continuous Monitoring

The continuous monitoring model assumes a network will not remain in a healthy state and it is therefore necessary to continuously review for faults. It further assumes devices and programs are designed to provide robust diagnostic information that can be logged and analyzed. Investment is focused on collecting and analyzing information from critical systems and network segments, identifying concerns, and alerting for further review and potential remediation.

A monitoring and logging guide authored by CREST, a U.K.-based non-profit cybersecurity organization, outlined a framework and process toward implementing continuous monitoring. Figure 4 illustrates the framework in which common logging mechanisms within a network are analyzed.[72] Such logs exist at the server, network, application, and security suite level. The seven-step process is to: 1) develop a

[69] "Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments," NSA, accessed August 21, 2016, 1, https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf.

[70] Joerg Hirschmann, "Defense in Depth: A Layered Approach to Network Security," *Security Magazine*, September 1, 2014, http://www.securitymagazine.com/articles/85788-defense-in-depth-a-layered-approach-to-network-security.

[71] Prescott E. Small, *Defense in Depth: An Impractical Strategy for a Cyber World* (Bethesda, MD: SANS Institute 2011), 6–7.

[72] Jason Creasey, *Cyber Security Monitoring and Logging Guide* (Berkshire, UK: CREST, 2015), 6.

monitoring and logging plan; 2) identify and address your cybersecurity posture outside of logging and monitoring; 3) identify sources of security indicators; 4) develop people, processes, and practices to monitor and log; 5) buy or build monitoring and logging solutions; 6) integrate solutions into security architecture; and 7) maintain the capability.[73]

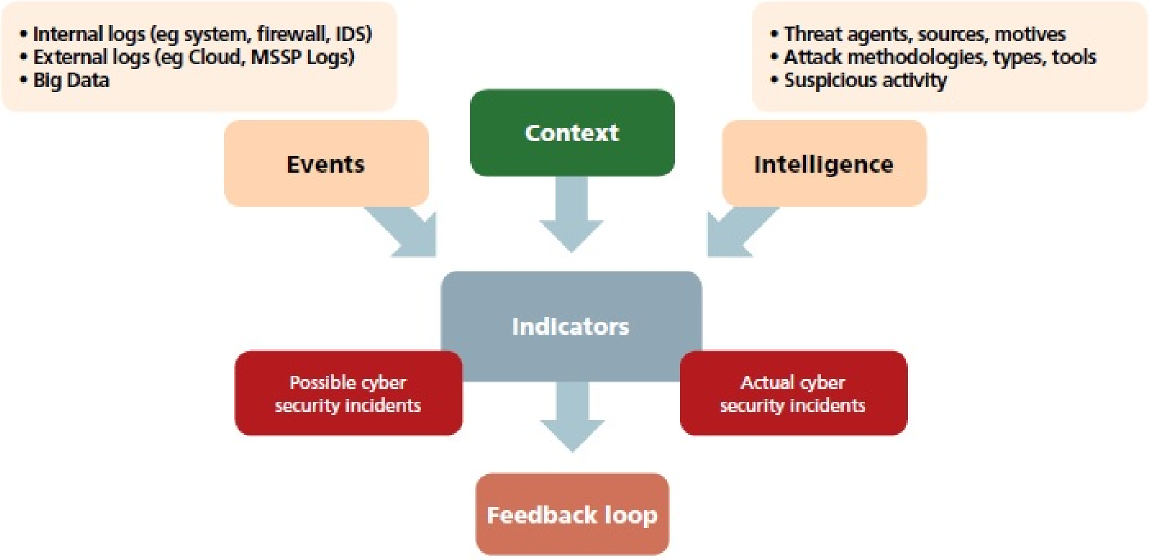

• Internal logs (eg system, firewall, IDS)
• External logs (eg Cloud, MSSP Logs)
• Big Data
• Threat agents, sources, motives
• Attack methodologies, types, tools
• Suspicious activity
Events
Context
Intelligence
Indicators
Possible cyber security incidents
Actual cyber security incidents
Feedback loop

Figure 4. CREST Monitoring and Logging Framework[74]

The main drawback of continuous monitoring is managing the complexity of information collected, and the level of effort required to synthesize the collected data into digestible information. The model also assumes devices and applications will generate sufficient logs to identify a fault. Finally, the model does not make explicit the remediation of incidents.

[73] Ibid., 53–59.

[74] Ibid., 6.

4. Intelligence-Driven

The intelligence-driven model attempts to understand cyber attacks using information about the aggressor. Motivation and attack life cycle are analyzed to assess points of vulnerability and defensive gaps. Lockheed Martin's Cyber Kill Chain framework implements this at the operational level. It consists of seven stages through which an attacker must successfully progress, with the belief that a defender can disrupt the attacker at any of the seven stages.[75] Adversary intelligence is collected and evaluated for each step toward identifying attack mitigation strategies. The seven stages of the Cyber Kill Chain are:

- Reconnaissance—the attacker identifies the victim's assets and potential vulnerabilities to exploit;
- Weaponization—the attacker develops tools and scripts to conduct the cyber attack;
- Delivery—the attacker deploys the tools and scripts previously developed, most likely remotely, toward the target;
- Exploitation—the attacker uses the tools and scripts to take advantage of a vulnerability in the attacked system;
- Installation—once unauthorized access is obtained, the attacker moves additional tools and scripts to the victim system(s) to further exploit the compromised network;
- Command and Control (C2)—the attacker remotely controls the tools and scripts, allowing him or her to further exploit the compromised network;
- Actions on Objectives—whether through exfiltration or destruction, the attacker affects his or her original goal for attacking the victim.[76]

Deloitte introduced a more strategic model, geared toward processing of data and information into actionable intelligence (see Figure 5). Key elements include the collection of diversified information feeds from within and outside the defending

[75] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1 (2011): 82.

[76] Ibid., 83–84.

organization, integrated with expert analysis in a relevant contextual framework, and used to inform both technical and business decision processes.

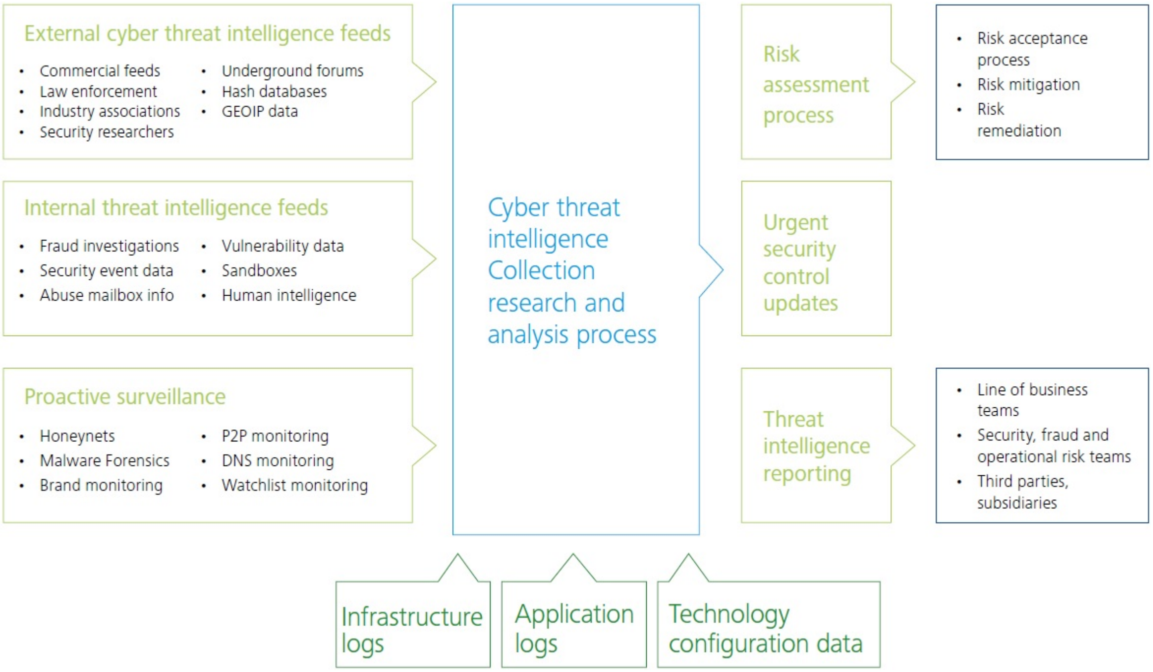


Figure 5. Deloitte Cyber Intelligence Model[77]

Despite its popularity, the Cyber Kill Chain has been criticized for focusing on malware and neglecting insider threat, social engineering, and non-malware remote access methods as the vector of intrusion.[78] Another critique of Deloitte’s model is that it relies upon considerable analytical resources for intelligence production, almost certainly far greater than available to most organizations.

[77] Stephane Hartaud, Laurent De La Vaissiere and Sebastien Besson, “Cyber Threat Intelligence, Move to a Cyber Intelligence-Driven Cybersecurity Model,” Deloitte, accessed September 17, 2016, 47, http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-cyber-threat-intelligence-cybersecurity-29102014.pdf.

[78] Giora Engel, “Deconstructing the Cyber Kill Chain,” Dark Reading, November 18, 2014, http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542.

C. KEY CYBERSECURITY EFFORTS

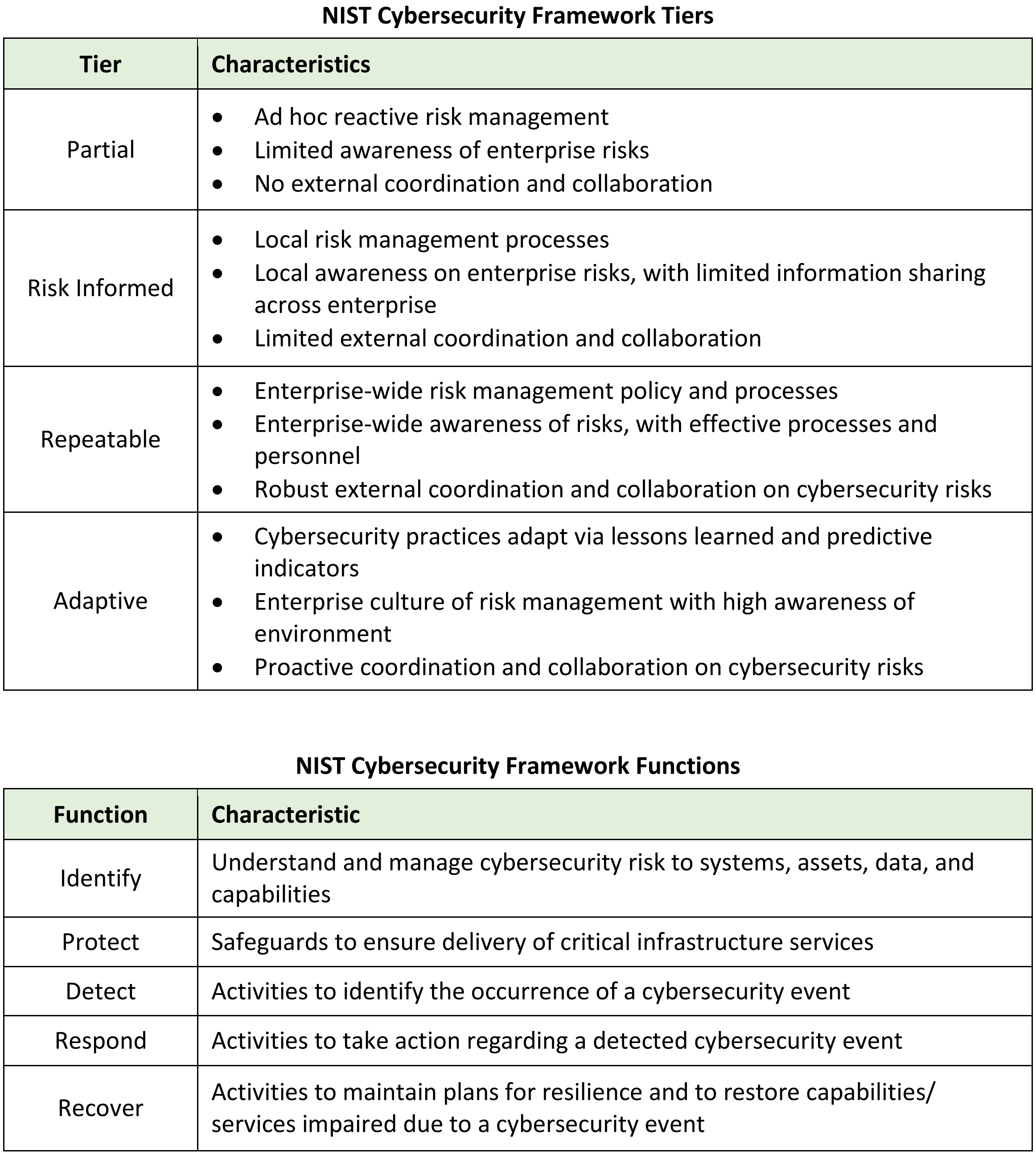
There has been considerable effort by the public and private sectors to address cybersecurity risks in today's environment. This section highlights four of the most influential efforts underway, designed to familiarize network defenders with the current threat environment. Most aspects of these are human driven, as they rely upon the synthesis of complex information toward subjective judgements.

1. NIST Cybersecurity Framework

In 2014, the National Institute of Standards and Technology (NIST), a branch of the U.S. Department of Commerce, published *Framework for Improving Critical Infrastructure Cybersecurity*, more popularly known as the NIST Cybersecurity Framework. The purpose of the framework is to understand, manage, and reduce cybersecurity risks by prioritizing activities to assure critical operations and service delivery.[79] It creates a common language to be used by cybersecurity professionals and executives that helps facilitate clearer communication when planning, implementing, and operating cybersecurity systems. The framework identifies four tiers of cybersecurity readiness with five core functions for effective cybersecurity (see Figure 6).[80] Together, these tiers and functions allow organizations to evaluate their readiness posture and to prioritize where investments can most optimally be made. NIST recommends organizations progress to at least tier three ("Repeatable") in their cybersecurity readiness.

[79] "Cybersecurity Framework Frequently Asked Questions," National Institute of Standards and Technology, last modified October 21, 2015, http://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics.cfm.

[80] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, MD: National Institute of Standards and Technology, 2014), 4–5.



NIST Cybersecurity Framework Tiers

Tier	Characteristics
Partial	• Ad hoc reactive risk management • Limited awareness of enterprise risks • No external coordination and collaboration
Risk Informed	• Local risk management processes • Local awareness on enterprise risks, with limited information sharing across enterprise • Limited external coordination and collaboration
Repeatable	• Enterprise-wide risk management policy and processes • Enterprise-wide awareness of risks, with effective processes and personnel • Robust external coordination and collaboration on cybersecurity risks
Adaptive	• Cybersecurity practices adapt via lessons learned and predictive indicators • Enterprise culture of risk management with high awareness of environment • Proactive coordination and collaboration on cybersecurity risks

NIST Cybersecurity Framework Functions

Function	Characteristic
Identify	Understand and manage cybersecurity risk to systems, assets, data, and capabilities
Protect	Safeguards to ensure delivery of critical infrastructure services
Detect	Activities to identify the occurrence of a cybersecurity event
Respond	Activities to take action regarding a detected cybersecurity event
Recover	Activities to maintain plans for resilience and to restore capabilities/ services impaired due to a cybersecurity event

Figure 6. NIST Cybersecurity Framework Tiers and Functions[81]

[81] Ibid., 8–11.

This framework encourages planned and well-resourced cybersecurity efforts, but falls short in fully integrating cyber threat intelligence. In an assessment of the framework conducted by PwC, they indicated that the framework "does not address the need to implement processes to identify and understand an organization's unique threat adversaries, their motivations, their capabilities, and the data they target."[82]

2. Automated Indicator Sharing

DHS, through the National Cybersecurity and Communications Integration Center (NCCIC), established the Automated Indicator Sharing (AIS) program to encourage real-time sharing of threat information between participants, which include federal, state, local, tribal, territorial, information sharing and analysis centers; private companies; and foreign partners.[83] AIS is built upon two complementary technical specifications developed internationally through community-driven collaboration, for the purpose of information sharing about cyber threats, situational awareness, and the defense of networks.[84]

One of these specifications is TAXII, which is an acronym for the Trusted Automated eXchange of Indicator Information, designed to facilitate the exchange of cyber threat information.[85] It is a framework to provide services, messaging and protocols, querying, and content categories.[86] The other specification is STIX, which is a structured language to convey the full range of cyber threat information. Examples include the analysis of threats, incidents, indicators, patterns of behavior, defensive response to threats, adversaries, and adversarial efforts.[87] To use an analogy around

[82] PricewaterhouseCoopers, *Why You Should Adopt the NIST Cybersecurity Framework* (New York: PricewaterhouseCoopers, 2014), 6.

[83] "Automated Information Sharing (AIS)," US-CERT, accessed August 27, 2016, https://www.us-cert.gov/ais.

[84] "Information Sharing Specifications for Cybersecurity," DHS, accessed July 13, 2016, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.

[85] Julie Connolly, Mark Davidson, and Charles Schmidt, *The Trusted Automated eXchange of Indicator Information (TAXII)* (Bedford, MA: MITRE Corporation, 2014), 3.

[86] Ibid., 6–7.

[87] MITRE, *Threat-Based Defense: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)* (Bedford, MA: MITRE Corporation, 2012), 5.

human language, TAXII is the phone and the voice networks we use to communicate, inclusive of services to connect people together; STIX is English, and all the rules that govern forming comprehensible phrases and sentences.

There has been some concern expressed over AIS, citing potential issues with customer privacy, PII leakage, unwanted scrutiny into vulnerabilities within participant networks, and potential legal liability.[88] Participation in AIS by private industry is also discretionary, both at the organizational and incident level. The timeliness and completeness of information can therefore not be assured.

3. Continuous Diagnosis and Mitigation

DHS also developed Continuous Diagnosis and Monitoring (CDM), an implementation of the NIST framework principles that charts a three-pronged strategy. The first prong is to harden the components throughout a network by authorizing and managing all capacity, capability, and users. The second is automated scanning of all managed devices and activities to provide more timely and enhanced situational awareness of security vulnerabilities throughout the network. The third is maturation of processes and tools to aid decision makers in their efforts to prioritize issues and mitigation strategies. When implemented, CDM provides cyber security professionals a comprehensive solution to manage cyber assets (see Figure 7). CDM is mandated for federal departments and agencies, and available for use by state, local, tribal, and territorial governments. As a program, it consists of a modernized security framework, a suite of over 300 commercial off-the-shelf technologies, and an acquisition tool to streamline purchasing and reduce costs.[89]

[88] Mary K. Pratt, "As Threats to Data Spread, Security Info Sharing Debate Heats Up," TechTarget, accessed August 28, 2016, http://searchcompliance.techtarget.com/feature/As-threats-to-data-spread-security-info-sharing-debate-heats-up.

[89] "CDM Product Catalog," DHS, last modified March 2016, http://www.gsa.gov/portal/mediaId/131294/fileName/GSA_CDM_ProductGuide_2016-03-11d.action.

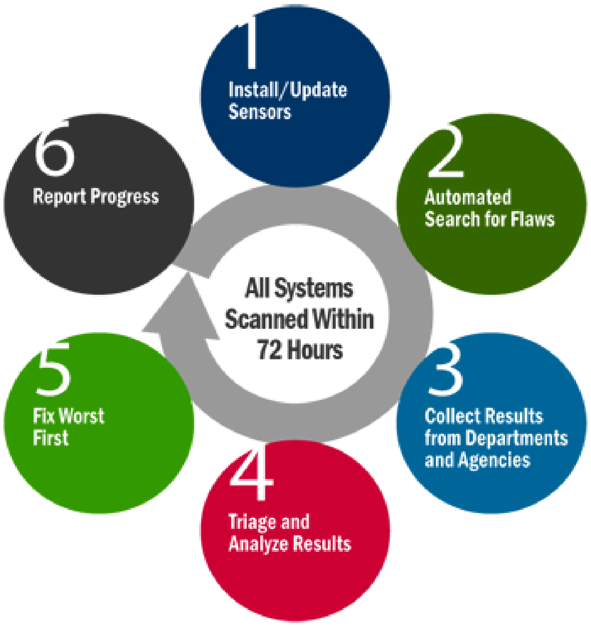

1
Install/Update Sensors
2
Automated Search for Flaws
3
Collect Results from Departments and Agencies
4
Triage and Analyze Results
5
Fix Worst First
6
Report Progress
All Systems Scanned Within 72 Hours

Figure 7. CDM Operational Model[90]

CDM's framework provides for an extensible security architecture. While it is fully defined by fifteen core functions, it has been segmented into three phases so it can be implemented over time.[91] Phase One focuses on cyber assets, both physical and logical, and addresses the issue of hardening individual devices. It includes identification of known malware instances, device configuration management, and introduction of new hardware and software into the environment. Phase Two focuses on the business processes and people the network serves. It manages access to accounts, services, and information available to authorized users, and identifies anomalies, flagging potential accidental, reckless, and malicious behaviors by insiders Phase Three addresses processes and practices to optimally manage the security life cycle of the network, including response to incidents. Phase Three accounts for the an organization's constantly changing environment, and changes to the systems that support the organization. As new business requirements are identified—then engineered into capabilities, capacity, processes, and

[90] John Pescatore, *Continuous Diagnostics and Mitigation: Making it Work* (Bethesda, MD: SANS Institute, 2014), 3.

[91] "CDM Capabilities," General Services Administration, last modified June 30, 2016, http://www.gsa.gov/portal/content/177887.

information resources—Phase Three integrates the requirements into the existing management structure established in Phases One and Two. Phase Three also builds a more robust, cohesive ability to plan, detect, and respond when things go wrong.

Similar to continuous monitoring, CDM has been criticized for being focused on vulnerabilities instead of threats, and offering an incomplete solution.[92] It also aims for a full three days from initiating a search for vulnerabilities to addressing them, which can be a very long time when an adversary is actively exploiting a network.

4. Active Cyber Defense

Consistent with its conceived use for national defense, the United States Department of Defense (DOD) proposed Active Cyber Defense (ACD) and described it within the *2011 DOD Strategy for Operations in Cyberspace*. The objective of ACD is to seize initiative from the attacker. DOD described ACD as "synchronized real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DOD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DOD networks and systems."[93] The strategy assumes that ACD will need to extend beyond a defender's network boundaries, with activities to understand the various threats to DOD networks.[94] The concept has been further developed by the National Security Agency's (NSA) Information Assurance Directorate (IAD), in which they defined six functional areas of ACD:

- Sensing—ability to monitor network environment, states, and behaviors;
- Sense-Making—analytics to understand events within context;
- Decision Making—reducing and evaluating response choices, and selecting the best option

[92] Richard Bejtlich, "Continuous Diagnostic Monitoring Does Not Detect Hackers," *TaoSecurity*, June 9, 2015, http://taosecurity.blogspot.com/2015/06/continuous-diagnostic-monitoring-does.html.

[93] DOD, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: DOD, 2011), 7.

[94] Ibid.

- Acting—affecting the selected choice, manually or automated;
- Messaging/Control—communication and coordination of shared situational awareness and responses;
- ACD Mission Management—operational control of any particular instance of an ACD implementation.[95]

Figure 8 illustrates the relationship between the first five functional areas (the sixth, ACD Mission Management, is not displayed as it is implementation dependent).

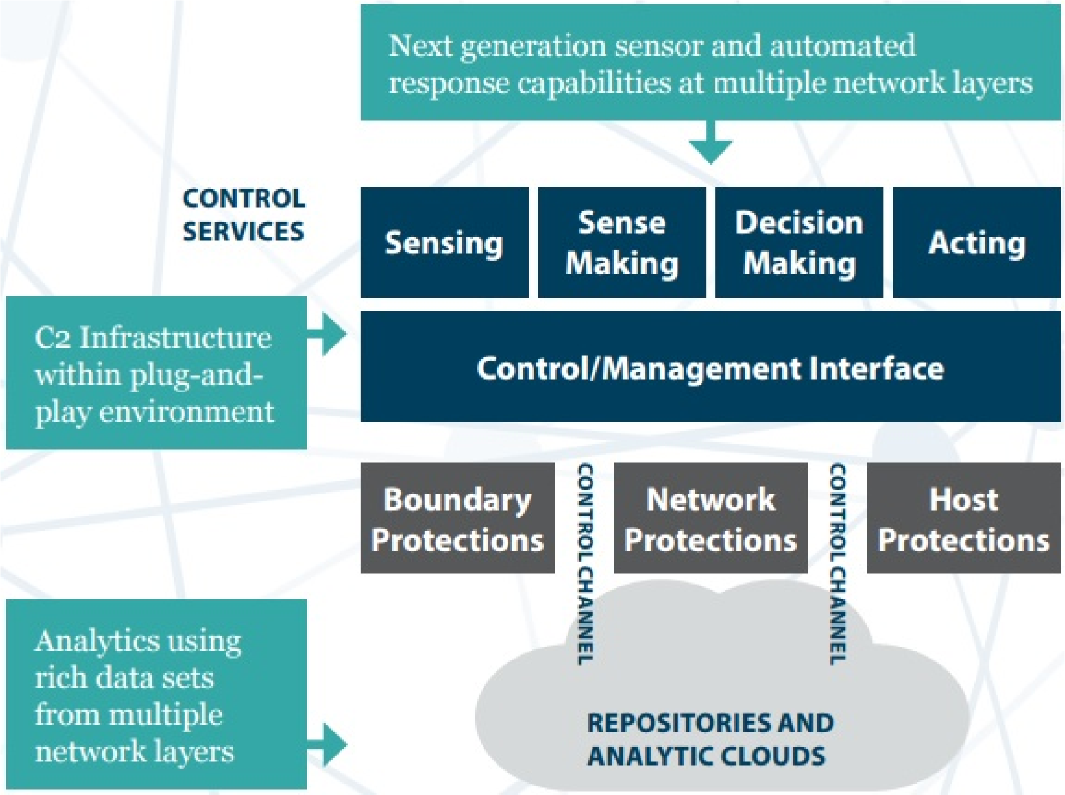

Next generation sensor and automated response capabilities at multiple network layers
CONTROL SERVICES
Sensing
Sense Making
Decision Making
Acting
C2 Infrastructure within plug-and-play environment
Control/Management Interface
Boundary Protections
CONTROL CHANNEL
Network Protections
CONTROL CHANNEL
Host Protections
Analytics using rich data sets from multiple network layers
REPOSITORIES AND ANALYTIC CLOUDS

Figure 8. NSA/IAD's ACD Conceptual Architecture[96]

[95] M. J. Herring and K. D. Willett, "Active Cyber Defense: A Vision for Real-Time Cyber Defense," *Journal of Information Warfare* 13, no. 2 (2014): 49–50.

[96] "Active Cyber Defense Fact Sheet," NSA, accessed July 13, 2016, https://www.iad.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm.

Those in the private sector have looked to leverage ACD concepts. Industry experts have not fully accepted the DOD's definition of ACD because of their own desires to mold the capability to non-defense purposes, despite the absence of legal authorities, protections, and obligations of sovereign nations. Emilio Iasiello, chief of threat analysis at iSIGHT Partners, argues there is no internationally agreed-upon definition of ACD.[97] A review of literature across academia, legal experts, industry experts, and government officials shows key characteristics of ACD applicable to private use. These characteristics are:

- is triggered by a malicious attack,
- involves knowledge of the defenders environment,
- provides mechanism for "near" real-time response, and
- provides mechanisms to respond, both internally and externally, to the defender's network.[98]

ACD techniques are built upon use of deception, disinformation, misdirection, delaying, deflection, attribution, degradation, and destruction.[99] Many of these have been researched and implemented into various tools available for private use. Within a defended network, available ACD tools include honeypots, honey patching, honeynets, honey files, decoys, tar pits, beacons, and traffic deflection. External to a defended network, the tools include deployment of remote access Trojans and other one-off hacking techniques to obtain information from, and possibly unauthorized access to, attacking systems.[100]

Significant challenges constrain private use of ACD techniques. Accurate identification of attackers remains an analytical art, complicating the decision of which

[97] Emilio Iasiello, "Hacking Back: Not the Right Solution," *Parameters* 44, no. 3 (2014): 1.

[98] Robert S. Dewar, "The Triptych of Cyber Security: A Classification of Cyber Defence," in *6th International Conference on Cyber Conflict (CyCon 2014)*, 9.

[99] Federico Araujo et al., "Experiences with Honey-Patching in Active Cyber Security Education," *8th Workshop on Cyber Security Experimentation and Test* (2015): 1, 2, 4; Anthony D. Glosson, *Active Defense: An Overview of the Debate and Way Forward* (Fairfax, VA: George Mason University, 2015), 5–6; Sean L. Harrington, "Cyber Security Active Defense: Playing with Fire or Sound Risk Management?" *Rich. JL & Tech.* 20 (2014): 17.

[100] Glosson, *Active Defense*, 6–7.

external systems to exploit when going after an attacker.[101] Further, the underlying back-and-forth between attackers and defenders requires constant innovation. Tools quickly become obsolete, requiring frequent and expensive reengineering. Additionally, lack of concise cyber laws and precedence has prevented consensus on the legality of its private use. The uncertainty of legality is expressed as opinion on the likelihood of criminal or civil liability for those engaged in ACD, with low risk for use of techniques within a defended network and high risk for use of techniques external to a defended network.[102] Further, the use of ACD techniques may result in individuals running afoul of professional ethics codes within the legal and cybersecurity fields.[103] Finally, external ACD techniques have a high likelihood of infringing upon the sovereign rights of nations, and may trigger geopolitical escalations with unintended consequences.[104]

[101] Dewar, "The Triptych of Cyber Security," 11.

[102] Ibid., 8–10.

[103] Harrington, "Cyber Security Active Defense," 5–6.

[104] Dewar, "The Triptych of Cyber Security," 8.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. AUTOMATED DEFENSE OF CYBER SYSTEMS

> [The next innovation regarding cybersecurity is] automating cybersecurity capabilities. Our networks and data are subject to continuous cyberattacks from a wide range of threats. Effective defenses against these adversaries include real-time, complex synchronization of thousands of endpoints and networks, multiple organizational processes, and the selection, de-confliction, and execution of complex response actions within and across diverse domains.
>
> —Curt Dukes, NSA/IAD Director

As previously argued, today's cybersecurity models and efforts will not be sufficient to address tomorrow's exponentially larger networks and corresponding vulnerabilities. The rate at which critical infrastructure, corporations, and citizens integrate IoT devices will upend current practices. However, it is possible to take today's concepts to build a more effective, scalable cybersecurity model. It requires tying cybersecurity to the same exponential growth curve as the technology it is bound to protect. This means responding to threats in cyber time, not human time, while avoiding offensive tools that may antagonize sovereign nations. Innovations are occurring that will propel automated solutions forward, and will come together into what is put suggested in this paper as automated defense of cyber systems (ADCS).

A. DEFINING ADCS

1. Automation

The definition of automation is fairly straightforward: "the technique, method, or system of operating or controlling a process by highly automatic (having the capability of starting, operating, moving, etc., independently) means, as by electronic devices, reducing human intervention to a minimum."[105] When applied to Director Curt Dukes' quote that opened this chapter, automating cyber defenses envisions protecting the networks and data from continuous attacks. Furthermore, the endpoints within networks

[105] "Automation," Dictionary.com, accessed August 1, 2016, http://www.dictionary.com/browse/automation.

matter—the individual devices are interconnected with each other, and these devices and networks support a variety of business operations critical for achieving an organization's mission. Automation includes assessing impact of deploying available defensive options on both the attacker and the defended network.

The timeframe for automation is "real-time," which is often quoted by cybersecurity experts. Don Adams, vice president and chief technology officer for TIBCO Software Federal, described a need to manage "real-time events from distributed sensors, agents and other processing components."[106] An analogous term is "cyber-relevant time."[107] The use of real and cyber-relevant time connotes that actions and reactions in cyberspace are the result of computation using algorithms, rather than application of human logic and judgement.[108] It does not imply instantaneous or immediate action. It is the amount of time necessary, which will vary depending upon an organization's mission, to support resiliency and smooth degradation such that defenders retain operational control over the defended devices and network.

Finally, the human is not completely removed from cybersecurity. Rather, automation is used to build a baseline of system-managed knowledge for use by cybersecurity professionals. The baseline of knowledge includes an understanding of the data traversing a network, devices and networks to be protected, knowledge of how business processes support business operations, means to measure and assess business operations, knowledge of what defensive options are available, and an ability to assess probable impact of defensive options on business operations.

2. ADCS Core Components

Future cybersecurity models must benefit from anticipated advancements in computational power and algorithms for the purpose of abstracting network and device complexity. Therefore, ADCS will build on top of advances in today's models and efforts

[106] Don Adams, *Predictive Cyber Defense—A Strategic Thought Paper* (Pal Alto, CA: TIBCO Software, 2010), 2.

[107] Herring and Willett, "Active Cyber Defense," 47.

[108] Jan Kallberg, "In Cyber, Time is of the Essence," *The Cyber Defense Review*, January 28, 2016, http://www.cyberdefensereview.org/2016/01/28/in-cyber-time-is-of-the-essence/.

that take advantage of enhanced structuring of information that currently feed human-driven processes. This will free cybersecurity professionals from the minutia of individual device management, allowing them to instead focus on supporting organizational objectives and resolving unanticipated cyber crises.

B. SENSORS

We have five senses—sight, hearing, taste, smell, and touch—to help us comprehend the world. ADCS will have senses as well, except many more than a person. Some of the ADCS senses will correlate to those possessed by humans while others will capture measurements relevant to cyber systems, such as network data flow. Others still will be geared toward measuring the operational mission of the network.

All of these senses will contribute to automated decision making. The importance of reading sensors and responding to them within automated cybersecurity systems was recognized in 2004 when two Institute of Electrical and Electronics Engineers (IEEE) members prototyped an autonomic defensive system, using the sensors to "repeatedly report on the presence or absence of normal or intrusive activity."[109]

1. The Sensing Device

Future sensors will have greater capability and autonomy than today's devices, enabled through miniaturization, self-power, and wireless communication. This will allow for their use in almost any conceivable environment enhanced through data processing.

Miniaturization is the ultimate win-win for electronics, as it allows for increased computational capacity at reduced power consumption. In the book *One-Dimensional Metals*, Sigmar Roth and David Carroll projected the minimum feature size of electronic components using a Moore plot. Examining transistor density, the book traced miniaturization from vacuum electronics, through solid-state, microelectronics, to VLSI (very large scale integration). The authors' projection culminates in the achievement of

[109] O. Patrick Kreidl and Tiffany M. Frazier, "Feedback Control Applied to Survivability: A Host-Based Autonomic Defense System," *IEEE transactions on Reliability* 53, no. 1 (2004): 149.

molecular electronics around the year 2020. The book also describes the technological challenges toward transitioning to the molecular level. While the realization of molecular transistors may not occur by 2020, the authors draw a plausible path for continued improvements.[110]

Dependence on reliable and continuous power further limits mass deployment of sensors. Unfortunately, the pace of battery development is frequently sighted as lagging the timescale described in Moore's Law.[111] Rather than relying on a slower-moving technology requiring recharge, advancements are being made in self-powered devices. In research conducted in 2003, two prototype systems were successfully developed using vibration-based magnetic coil generators, although the prototypes were large and clunky.[112] More recent work conducted in China prototyped self-powered smart skin, capable of detecting contact location and velocity, and sensitive enough to "perceive the perturbation of a honey bee," all on a 1.9 mm deep device.[113]

A research group from the Georgia Institute of Technology's School of Material Science described its wireless nanotechnology goal as "aiming at building a self-powered system that operates independently, sustainably, and wirelessly by itself without using a battery."[114] Their tests demonstrated a device capable of transmitting within a range of five to ten feet, with signals detectable using commercial radios.[115] Range limitations can be overcome through current protocols, such as Bluetooth, allowing signal retransmission over longer distances.[116]

[110] Siegmar Roth and David Carroll, *One-Dimensional Metals: Conjugated Polymers, Organic Crystals, Carbon Nanotubes and Graphene* (John Wiley & Sons, 2015): 193–210.

[111] Fred Schlachter, "No Moore's Law for Batteries," *Proceedings of the National Academy of Sciences* 110, no. 14 (2013): 5273.

[112] E. P. James et al., "An Investigation of Self-Powered Systems for Condition Monitoring Applications," *Sensors and Actuators A: Physical* 110, no. 1 (2004): 175.

[113] Mayue Shi et al., "Self-Powered Analogue Smart Skin," *ACS Nano* 10, no. 4 (2016): 4088.

[114] Youfan Hu et al., "Self-Powered System with Wireless Data Transmission," *Nano letters* 11, no. 6 (2011): 2572.

[115] Ibid., 2576.

[116] "Using Bluetooth for Data Communications in Industrial Automation," Digi-Key Electronics, April 25, 2013, http://www.digikey.com/en/articles/techzone/2013/apr/using-bluetooth-for-data-communications-in-industrial-automation.

2. Sensor Arrays

Equally important to individual sensor development is the ability for a large number of sensors to work in aggregate to develop high-resolution information. A group from the University of Texas Electrical Engineering Department demonstrated a massively-deployable architecture of sensor nodes, each capable of up to thirty-one distinct sensing capabilities. Similar to the wireless capabilities described in the previous section, the sensor array utilized low-power Bluetooth to wirelessly transmit to a base station, with the data transmitted over the internet and stored in the cloud.[117]

An advantage of large sensor arrays is that they are fault tolerant when one sensor fails. The readings of a particular sensor can be assessed relative to its neighbors to come to a judgment about the sensor's reliability. A 2006 research project utilized evolvable hardware (EHW), which applies genetic algorithms to programmable portions of the hardware. In the project, EHW was used to allow for autonomous reprogramming once a sensor fault was detected. This allowed for the removal of a node without human intervention, and without significantly detracting from measurement accuracy.[118]

3. Data Collection and Aggregation

The mass promulgation of sensors will inevitably result in data stores that are in orders of magnitude larger than they are today. Research on data from ambient assisted living communication (AAL) described this as a threefold problem: volume—large and/ or computationally heavy data sets; velocity—the rate at which data flow through the data store; and variety—the range of types and sources of data.[119] The solution proposed in the research is the use of metric space–based big data abstraction for computationally

[117] Cuong M. Nguyen et al., "Wireless Sensor Nodes for Environmental Monitoring in Internet of Things," *2015 IEEE MTT-S International Microwave Symposium*: 1–4.

[118] James M. Hereford, "Fault-Tolerant Sensor Systems using Evolvable Hardware," *IEEE Transactions on Instrumentation and Measurement* 55, no. 3 (2006): 846–853.

[119] Rui Mao et al., "Overcoming the Challenge of Variety: Big Data Abstraction, the Next Evolution of Data Management for AAL Communication Systems," *IEEE Communications Magazine* 53, no. 1 (2015): 42.

simpler analysis. The key is in engineering algorithms in which resulting data patterns could be recognized and understood.[120]

C. AUTONOMIC COMPUTING

When applied to cybersecurity, the goal of autonomic computing is development of technology to manage technology, abstracting a system's complexity while ensuring optimal performance.[121] IBM released a blueprint for a system and described four key attributes for autonomic computing.: self-configuring—dynamic adaptation to the environment; self-healing—discover, diagnose, and react to disruptions; self-optimizing—monitor and tune performance; and self-protecting—anticipate, detect, and counter all source threats.[122] A potential future for these four attributes is described in the following sections.

1. Self-Configuring, Healing, and Optimizing

In their review of over 1,100 articles about autonomic systems, Muccini, Sharaf, and Weyns found that the top priorities of autonomic research are efficiency/performance (i.e., self-optimizing), flexibility and reliability (i.e., self-healing), and configurability (i.e., self-configuring). Proposed autonomic solutions existed across the TCP/IP stack, with most existing at the application layer. A drawback identified by the review was that relatively few articles identified cybersecurity as the primary focus.[123]

In prototyping an autonomic architecture, Kreidl and Frazier defined four key architectural elements: the information system (i.e., host or device) to be protected, a set of sensors, a set of actuators capable of responding with various defensive mechanisms,

[120] Ibid., 44.

[121] Margaret Rouse, "Autonomic Computing," WhatIs, accessed July 13, 2016, http://whatis.techtarget.com/definition/autonomic-computing.

[122] IBM, *An Architectural Blueprint for Autonomic Computing* (Hawthorne, NY: IBM, 2005), 3.

[123] Henry Muccini, Mohammad Sharaf, and Danny Weyns, "Self-Adaptation for Cyber-Physical Systems: A Systematic Literature Review," *Proceedings of the 11th International Workshop on Software Engineering for Adaptive and Self-Managing Systems* (2016): 77.

and a controller to analyze and coordinate the sensors and actuators toward host survivability.[124]

Autonomic computing extends beyond the device, and must be able to handle increases in size, complexity, and topography of a network. It begins with an automated understanding of connected devices, their capabilities, and the communication channels that make up the whole. In a 2014 study of industrial control network awareness, Vollmer, Manic, and Linda developed a discovery mechanism they called Network Entity Identification (NEI). It used sensors to passively monitor network traffic for the purpose of identifying connected devices as well as correlating the logical and physical device addresses.[125] A more comprehensive solution will discover and catalog device capabilities, correlating them to business functions served by a network. With this in place, cybersecurity professionals will no longer manage the minutia of securing individual devices.

2. Self-Protecting

The defining characteristics of a self-protecting device, as suggested by Inderpreet Chopra in his dissertation, are that it can “proactively detect and identify hostile behavior and can take autonomous actions to defend itself.”[126] Chopra goes on to define a classification for a grid security system, identifying a hierarchy of attacks across the system, management, and network layers. He then describes various available techniques and algorithms, and proposes methods to detect and respond to such attacks across the system, management, and network levels.[127]

In 2016, four researchers at the University of Toronto published an article on Talos, a system designed to rapidly respond to coding flaws. A common line of threat for

[124] Kreidl and Frazier, “Feedback Control Applied to Survivability,” 149.

[125] Todd Vollmer, Milos Manic, and Ondrej Linda, “Autonomic Intelligent Cyber-Sensor to Support Industrial Control Network Awareness,” *IEEE Transactions on Industrial Informatics* 10, no. 2 (2014): 1652.

[126] Inderpreet Chopra, “Autonomic Model for Self-Healing and Self-Protection in Grid Computing using Multi-Agents,” (PhD diss., Thapar University, Patiala, 2015), 12.

[127] Ibid, 37–50.

systems is the pre-patch window of vulnerability where a specific vulnerability is identified and made public, but no fix is available.[128] What the University of Toronto researchers tested was a mechanism to trigger preexisting error-handling within vulnerable sections of code, thereby avoiding its execution and potential exploitation.[129] The mechanism demonstrated an ability to safely neutralize three-quarters of all potential vulnerabilities tested.[130] While this did result in loss of functionality, in most cases it was in non-critical portions of the software and did not prevent the product from performing its primary purpose.[131] When combined with a sensing network, this technique could be integrated and deployed as one of multiple options to mitigate a threat attempting to manifest itself on a device.

An example of a self-protection mechanism beyond a single device is the automated creation of internal decoys and disinformation in response to a cyber attack. The idea is that an autonomic system could handle the complexity of extending the defended network by creating realistic and compartmentalized segments. The intent would be to distract, confuse, and mitigate the efforts of the attacker. Jonathan Voris, Jill Jermyn, Nathanial Boggs, and Salvatore Stolfo prototyped a technique to automate the deployment of decoy files within a network, verifying that the system was as effective as manual generation and placement of such files.[132] In the study cited in the previous section, Vollmer, Manic, and Linda integrated a dynamic honeypot defense and demonstrated a capability to "automatically deploy deceptive virtual network entities" for the purpose of luring those conducting a cyber attack.[133]

[128] Zhen Huang et al., "Talos: Neutralizing Vulnerabilities with Security Workarounds for Rapid Response," *2016 IEEE Symposium on Security and Privacy*: 618.

[129] Ibid., 619.

[130] Ibid., 629.

[131] Ibid., 631.

[132] Jonathan Voris et al., "Fox in the Trap: Thwarting Masqueraders via Automated Decoy Document Deployment," *Proceedings of the Eighth European Workshop on System Security* (2015): 3.

[133] Vollmer, Manic, and Linda, "Autonomic Intelligent Cyber Sensor," 1652.

D. ARTIFICIAL INTELLIGENCE

Tim Urban, a prolific writer on the topic of AI, divides AI's evolution into three tiers. The first is Artificial Narrow Intelligence (ANI), described as specialization in one area, but not extendable or applicable in other domains (like asking a self-driving car to play chess, which it would never learn to do). The second, Artificial General Intelligence (AGI), possesses a capability on par with human intelligence; it can be given any task, and incorporates the ability to reason, abstract, and learn from experience. The third, Artificial Superintelligence, is the creation of an intellect superior to humans, and is the type of AI that generates the greatest speculation on existential impact, positive or negative.[134]

This thesis focuses on potential solutions in the ANI space. ANI is the area of AI where innovations are already available today, and where rapid growth over the next ten to fifteen years is most likely to occur.

1. Machine Learning

Machine learning is a sub-domain of AI that automates the process of "getting computers to act without being programmed," and incorporates training techniques both supervised and unsupervised by humans.[135] The technology has been applied to problem solving in a number of areas, a few of which include face detection, identification of topics within articles, and medical diagnosis.[136]

Northrup Grumman developed a system called BluVector, designed to utilize machine learning to better detect and classify malicious software in real-time operating in a network.[137] An independent test of BluVector's efficacy, conducted by Miercom, achieved malware detection rates between 99 and 100 percent across multiple tests, and

[134] Ibid.

[135] Andrew Ng, "Machine Learning," Coursera, accessed August 28, 2016, https://www.coursera.org/learn/machine-learning.

[136] Rob Schapire, "COS 511: Theoretical Machine Learning," Princeton University, Lecture Notes, February 4, 2008, http://www.cs.princeton.edu/courses/archive/spr08/cos511/scribe_notes/0204.pdf.

[137] Northrop Grumman, *BluVector: Applying Machine Learning Techniques to Achieve Resilient, Accurate, High-Speed Malware Detection* (Falls Church, VA: Northrup Grumman Corporation, 2014).

was complementary to BluVector's logging system and how it can be used in threat remediation.[138] Crowdstrike has introduced a similar system called Falcon Host, a product with its own machine learning algorithms.[139] A challenge for unsupervised machine learning is false-positive rate, which rises with detection rate and is a source of great frustration to defenders by mixing real attacks with suspect but innocuous events. To address this, a group from MIT developed the AI^2 platform, which combines supervised and unsupervised machine learning techniques. Analyzing 3.6 billion log lines, the system was able to achieve a cyber attack detection rate of greater than 86 percent while reducing the rate of false positives by 500 percent.[140]

2. Situational Awareness

One of the challenges in today's cyberspace environment is building situational awareness, which Endsley describes as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of the status in the near future."[141] MITRE goes on to describe three sub-domains of cyber situational awareness: network, threat, and mission awareness. These in turn feed into providing a tactical, operational, and strategic outlook for decision making.[142]

Because of the overwhelming amount of information to consider, the problem space requires computational assistance to collate and synthesize in a timely manner. In a 2014 literature review of cyber situational awareness, Franke and Brynielsson identified 102 articles dedicated to building cyber situational awareness. Of those, they found 45

[138] Miercom, *BluVector Cyber Threat Detection and Hunting Program* (East Windsor, NJ: Miercom, 2016), 3.

[139] Jackie Castelli, "How to Prevent Malware Infections with Machine Learning in Crowdstrike Falcon Host," *Crowdstrike Blog*, July 27, 2016, https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon-host-machine-learning/.

[140] Kalyan Veeramachaneni et al., "AI^2: Training a Big Data Machine to Defend," accessed September 17, 2016, 1–2, https://people.csail.mit.edu/kalyan/AI2_Paper.pdf.

[141] M. R. Endsley, "Design and Evaluation for Situation Awareness Enhancement," *Proceedings of the Human Factors Society 32nd Annual Meeting* (1988): 97–101.

[142] "Cybersecurity: Situational Awareness," MITRE, accessed August 8, 2016, https://www.mitre.org/capabilities/cybersecurity/situation-awareness.

with an empirical contribution, described as having "results based on data from experiments or archival studies, but also e.g., mathematical proofs, results from simulations, informed reasoning about computational complexity etc."[143] Further, 33 of those articles contained ideas for design and implementation. This demonstrates potential for significant advancement of ANI situational awareness tools for network defense.

3. Dealing with Uncertainty

As inter- and intra-network complexity increases, wicked problems will present themselves with greater frequency. A cyber attack and corresponding defensive cybersecurity response, whether performed manually or automated, may upset the homeostatic state of a network. ADCS needs to measure and assess the effects of attacker and defender actions, which include actual and relative changes in network status and their impact on supported business processes.

In a 2015 article, Zoubin Chahramani from the University of Cambridge described a framework utilizing probabilistic modeling applied to machine learning, with a goal of allowing computers to learn from observing data made available to them. However, data by nature is incomplete, either due to a lack of collection or granularity. Machine learning relies on making assumptions, or inferences, about unobserved data from the observed data, and the collection of assumptions is represented in a model. Uncertainty is the expression of that model's inability to accurately predict unobserved data. Probabilistic modeling captures and accounts for all uncertainty within a model using probabilistic distributions, and "learns" through the use of Bayesian learning to adjust the distribution after observing new data.[144]

4. Human Analogy

An analogy of ADCS to human biology is made to illustrate the relationship of the ADCS components to the desired cybersecurity capability. The analogy has been

[143] Ulrik Franke and Joel Brynielsson, "Cyber Situational Awareness—A Systematic Review of the Literature," *Computers & Security* 46 (2014): 18–31.

[144] Zoubin Ghahramani, "Probabilistic Machine Learning and Artificial Intelligence," *Nature* 521, no. 7553 (2015): 452–459.

frequently used in the literature to address complexity and visualize solutions. In a 2009 IEEE article, the autonomous nervous system was used as a model to build a cybersecurity architecture. It accounted for sympathetic (unconscious) and parasympathetic (conscious) actions, which sometimes conflict with each other but are complementary toward achieving homeostasis in protecting the body.[145] For example, the body unconsciously breathes, but breathing can be controlled when it can be harmful, such as when one is underwater or in a smoke-filled room.

In ADCS, sympathetic actions are automated while parasympathetic actions are controlled by cybersecurity professionals. The ADCS components make up the lower- and higher-order elements of a complex system, much like nerves and organs make up the body. ADCS is self-contained in that the defensive mechanisms are focused internal to the defended network. The concept of an internally defended network was introduced by Dr. Kristopher Hall when he built and tested Rx, a cyber security system to mitigate threats from internet worms. Rx looked at cyber security threats as a disease, and used concepts from biological epidemiology to internally treat them.[146]

[145] Vollmer, Manic, and Linda, “Autonomic Intelligent Cyber-Sensor,” 1648.

[146] Kristopher Joseph Hall, “Thwarting Network Stealth Worms,” (PhD diss., Virginia Polytechnic Institute and State University, 2006), 2.

V. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

A. FINDINGS

This thesis began by considering if automated cyber defense promises to be more effective than current models in coping with anticipated exponential growth of IoT devices and vulnerabilities, and subsequently examined relevant literature. An affirmative response was validated through the examination of the present and future cybersecurity landscape.

The IoT wave began in earnest in the early part of the current decade, and there is no reason to believe it will abate from exponential growth. Additionally, the internet has shown to be inherently insecure since its inception, with new vulnerabilities introduced and identified on a regular basis. Terrorism, nation states, and organized crime will continue to be the three primary malicious actors, and the level of threat from them may even grow as the cost to conduct offensive cyber operations drops while the cost to defend increases. Consequently, there will be a greater surface area with vulnerabilities exploitable by those motivated to attack.

Defensive models have evolved since the inception of the internet, beginning with a simplistic exterior network defense, progressing to layered, ever vigilant, and intelligence driven. Both industry and government have adapted to increasingly complex networks, setting frameworks for establishing defensive efforts, exchanging attack intelligence, and moving toward partial automation. Broad use of external/offensive cyber operations is not viable, particularly by private industry, as it has high business and professional risks, introduces the potential for criminal liability, and may lead to unintended escalation between nation states.

B. CONCLUSIONS

Greater automation is viewed as the future of cyber defense. Numerous technological advantages are on the near-to-mid horizon to help perform many cybersecurity functions. They will take advantage of the same exponential growth curve as seen in the introduction of IoT devices, thereby allowing a slowly growing number of cybersecurity professionals to defend vastly larger and more complex networks.

A vast decrease in price with corresponding increase in computational power will be the driving force behind mass deployment of internet-enabled sensors. This will make a sea of data available for use by automated cyber defensive systems that are capable of responding at both the device and network level. These sensors will feed into AI systems tuned to maximize the performance of the network while handling configuration, healing, optimization, and protection activities under most circumstances. Cybersecurity professionals will remain involved by monitoring and tuning AI systems, and to step in when circumstances arise that cannot be handled by automated systems. The automation and abstraction provided by ADCS will allow private industry to limit the number of cybersecurity professionals they will need to hire. The skillset and experience required by cybersecurity professionals will increase, as they will be expected to understand defensive AI systems as well as modeling of business functions supported by networks.

C. RECOMMENDATIONS

The realization of ADCS will not take place overnight. It is much more likely it will arrive piecemeal, with incremental improvements to the sensor, autonomic, and AI components.

National policy should continue to encourage investment in the broad use of defensive cyber automation. Such automation should be limited to activities contained within a defender’s network, and should not include offensive cyber measures in which the CIA triad is compromised without authorization. The reasons are threefold. First, offensive cyber measures introduce unacceptable risk to the businesses and individuals conducting the offensive operations. Second, the actions performed will likely be transnational, may not reflect the will or interests of the United States, and will not have the same accountability to the governed as cyber actions initiated by the government. Third, automated cyber attacks beyond human control, even for defensive purposes, may result in magnified real-world consequences that are rapidly escalated and unintended.

When considering incremental improvements from today's cyber security environment, a logical first step is to provide the advantages of CDM to private industry. While the U.S. government provides some incentive through mandating adoption and use by executive agencies, private industry represents the greatest source of funding available to encourage more research and faster product development. Further, private industry's use and contribution to cyber vulnerability and threat information sharing is critical, and barriers to participation in the Automated Indicator Sharing program should be aggressively removed, whether through incentives, regulatory control, or mitigation of civil liability.

Finally, organizations should develop an investment strategy in building sensor networks that support operations. This encompasses evaluation and iteration of data useful for collection. Likewise, they should invest in development and maturation of computational models that capture business functions. Rather than trying to model entire systems, such development should be incremental, focusing on the most critical business processes, data sets, or network segments. This, in turn, will feed into improvements in automation.

D. FUTURE RESEARCH

Future areas for research toward ADCS realization are plentiful. Unexplored, but implied and interrelated to the benefits of ADCS, are the mitigation of non-malicious cyber disruptions, which can include such things as hardware, software, and human operator failures. Benefits of system reliability and resiliency may prove to be far greater for non-malicious incidents than for malicious ones.

While the paper evaluated the vulnerabilities and threats faced by cyber networks through the introduction of vulnerabilities by IoT devices, the complexity of cyber-physical systems (CPS) and their impact on social networks was not explored. It is highly likely that future networks will support CPS, and successful cyber attacks may increasingly cause non-virtual effects experienced by more people. This may alter the consequence piece of the risk calculus, and potentially support more urgent action on cyber defense.

This thesis did not consider the use of non-cyber deterrents to malicious activity. Anecdotal observations from recent legal actions by the U.S. Department of Justice against PRC and Iranian cyber actors suggest an evolution of state-sponsored activities. A targeted study of state behavior pre- and post-indictment would be of interest toward understanding the evolution of threat actor motivations. The indictments may also be influencing how states view norms of cyber behavior, which have yet to crystalize into formal agreements of treaties.

Finally, this thesis speculated on only a few technologies that may shape the cybersecurity environment. There are undoubtedly more techniques and algorithms beyond sensors, autonomics, and AI that will emerge as viable cybersecurity solutions over the next ten to fifteen years.

LIST OF REFERENCES

Adams, Don. “Predictive Cyber Defense—A Strategic Thought Paper.” Pal Alto, CA: TIBCO Software, 2010.

Araujo, Federico, Mohammad Shapouri, Sonakshi Pandey, and Kevin Hamlen. “Experiences with Honey-Patching in Active Cyber Security Education.” Presented at the 8th Workshop on Cyber Security Experimentation and Test, Washington, DC, August 10, 2015.

Ashford, Warwick. “Exploding IoT attack surface Not an Immediate Threat to Business.” ComputerWeekly. May 27, 2016. http://www.computerweekly.com/news/450297327/Exploding-IoT-attack-surface-not-an-immediate-threat-to-business.

AT&T. “The CEO’s Guide to Security the Internet of Things.” 2016. https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf.

Bejtlich, Richard. “Continuous Diagnostic Monitoring Does Not Detect Hackers.” TaoSecurity. June 9, 2015. http://taosecurity.blogspot.com/2015/06/continuous-diagnostic-monitoring-does.html.

Bonderud, Douglas. “IoT Warning: FBI Says More Devices Equal Bigger Attack Surface.” Security Intelligence. Last modified September 15, 2015. https://securityintelligence.com/news/iot-warning-fbi-says-more-devices-equal-bigger-attack-surface/.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, and Steve Chon. “Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime.” *International Journal of Cyber Criminology* 8, no. 1 (2014).

Castelli, Jackie. “How to Prevent Malware Infections with Machine Learning in Crowdstrike Falcon Host.” Crowdstrike Blog. July 27, 2016. https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon-host-machine-learning/.

Chelf, Ben. Measuring Software Quality, A Study of Open Source Software. San Francisco: Coverity, 2006. http://www.coverity.com/library/pdf/open_source_quality_report.pdf.

Chia, Terry. “Confidentiality, Integrity, Availability: The Three Components of the CIA Triad.” *IT Security Community Blog*. August 20, 2012. http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/.

Chopra, Inderpreet. “Autonomic Model for Self-Healing and Self-Protection in Grid Computing using Multi-Agents.” PhD diss., Thapar University, Patiala, 2015.

Christensen, Clayton M. “Exploring the Limits of the Technology S-curve. Part I: Component Technologies.” *Production and Operations Management* 1, no. 4 (Fall 1992): 334–357.

Cid, Daniel. “Large CCTV Botnet Leveraged in DDos Attacks.” sucuri. June 27, 2016. https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html.

CompTIA. “Sizing up the Internet of Things.” August 28, 2015. https://www.comptia.org/resources/sizing-up-the-internet-of-things.

Concise AC. “Hacker Tools Top Ten: Our Recommended Tools for 2016.” Accessed August 26, 2016. https://www.concise-courses.com/hacking-tools/top-ten/.

Connolly, Julie, Mark Davidson, and Charles Schmidt. *The Trusted Automated eXchange of Indicator Information (TAXII)*. Bedford, MA: MITRE Corporation, 2014.

Creasey, Jason. *Cyber Security Monitoring and Logging Guide*. Berkshire, UK: CREST, 2015.

Crowdstrike. “2015 Crowdstrike Global Threat Report.” Accessed August 21, 2016. https://www.crowdstrike.com/global-threat-report-2015/.

Dell SecureWorks. “Underground Hacker Markets.” 2016. https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace.* Washington, DC: DOD, 2011.

Department of Homeland Security. “CDM Product Catalog.” Last modified March 2016. http://www.gsa.gov/portal/mediaId/131294/fileName/GSA_CDM_ProductGuide_2016-03-11d.action.

———. “Information Sharing Specifications for Cybersecurity.” Accessed July 13, 2016. https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.

Department of Labor Bureau of Labor Statistics. “Occupational Outlook Handbook: Information Security Analyst.” December 17, 2015. http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

———. “Occupational Outlook Handbook: Network and Computer Systems Administrators.” December 17, 2015. http://www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm.

Digi-Key Electronics. “Using Bluetooth for Data Communications in Industrial Automation.” April 25, 2013. http://www.digikey.com/en/articles/techzone/2013/apr/using-bluetooth-for-data-communications-in-industrial-automation.

Ding, Jianguo. “Intrusion Detection, Prevention, and Response System (IDPRS) for Cyber-Physical Systems (CPSs).” In *Securing Cyber-Physical Systems*. Edited by Al-Sakib Khan Pathan. Boca Raton, FL: CRC Press, 2015.

Endsley, M. R. “Design and Evaluation for Situation Awareness Enhancement.” *Proceedings of the Human Factors Society 32nd Annual Meeting* (1988): 97–101.

Engel, Giora. “Deconstructing the Cyber Kill Chain.” Dark Reading. November 18, 2014. http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542.

Federal Bureau of Investigation. “Going Dark.” Accessed July 29, 2016. https://www.fbi.gov/services/operational-technology/going-dark.

———. “International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector.” March 24, 2016. https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector.

FireEye. “Redline Drawn: China Recalculates its Use of Cyber Espionage.” Accessed August 21, 2016. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Franke, Ulrik, and Joel Brynielsson. “Cyber Situational Awareness—A Systematic Review of the Literature.” *Computers & Security* 46 (2014): 18–31.

Gartner. “Forecast Analysis: Information Security, Wordwide, 4Q15 Update.” March 22, 2016. https://www.gartner.com/doc/3261517/forecast-analysis-information-security-worldwide.

———. “Gartner says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach 75.4 Billion in 2015.” September 23, 2015. http://www.gartner.com/newsroom/id/3135617.

General Accounting Office. *Information Security: Technologies to Secure Federal Systems* (GAO-04-467). Washington, DC: General Accounting Office, 2004.

General Services Administration. “CDM Capabilities.” Last modified June 30, 2016. http://www.gsa.gov/portal/content/177887.

Ghahramani, Zoubin. “Probabilistic Machine Learning and Artificial Intelligence.” *Nature* 521, no. 7553 (2015): 452–459.

Gioria, Sebastien. “CLUSIRInfoNord OWASP IoT 2014.” LinkedIn. January 20, 2015. http://www.slideshare.net/SebastienGioria/clusir-infonord-owasp-iot-2014.

Glosson, Anthony D. *Active Defense: An Overview of the Debate and Way Forward*. Fairfax, VA: George Mason University, 2015.

Graham, Bradley. “Military Grappling with Rules for Cyber Warfare.” Washington Post. November 8, 1999. http://www.washingtonpost.com.

Northrop Grumman. *BluVector: Applying Machine Learning Techniques to Achieve Resilient, Accurate, High-Speed Malware Detection*. Falls Church, VA: Northrup Grumman Corporation, 2014.

Hall, Kristopher Joseph. “Thwarting Network Stealth Worms.” PhD diss., Virginia Polytechnic Institute and State University, 2006.

Harrington, Sean L. “Cyber Security Active Defense: Playing with Fire or Sound Risk Management?” *Rich. JL & Tech.* 20 (2014).

Hartaud, Stephane, Laurent De La Vaissiere and Sebastien Besson. “Cyber Threat Intelligence, Move to a Cyber Intelligence-Driven Cybersecurity Model.” Deloitte. Accessed September 17, 2016. http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-cyber-threat-intelligence-cybersecurity-29102014.pdf.

Henry, Shawn. “Cyber Threat: On the Front Lines with Shawn Henry.” Federal Bureau of Investigation. March 27, 2012. https://ucr.fbi.gov/news/stories/2012/march/shawn-henry_032712/shawn-henry_032712.

Hereford, James M. “Fault-Tolerant Sensor Systems using Evolvable Hardware.” *IEEE Transactions on Instrumentation and Measurement* 55, no. 3 (2006): 846–853.

Herring, M. J., and K. D. Willett. “Active Cyber Defense: A Vision for Real-Time Cyber Defense.” *Journal of Information Warfare* 13, no. 2 (2014).

Hewlett Packard Enterprise. “Internet of Things Research Study.” November 2015. https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

Hirschmann, Joerg. “Defense in Depth: A Layered Approach to Network Security.” Security Magazine. September 1, 2014. http://www.securitymagazine.com/articles/85788-defense-in-depth-a-layered-approach-to-network-security.

Hoffman, Chris. “Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats.” How-To Geek. April 20, 2013. http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/.

Hu, Youfan, Yan Zhang, Chen Xu, Long Lin, Robert L. Snyder, and Zhong Lin Wang. "Self-Powered System with Wireless Data Transmission." *Nano Letters* 11, no. 6 (2011).

Hua, Jian, and Sanjay Bapna. "The Economic Impact of Cyber Terrorism," *The Journal of Strategic Information Systems* 22, no. 2 (2013).

Huang, Zhen, Mariana D'Angelo, Dhaval Miyani, and David Lie. "Talos: Neutralizing Vulnerabilities with Security Workarounds for Rapid Response." 2016 IEEE Symposium on Security and Privacy, May 23–25, San Jose, CA.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Leading Issues in Information Warfare & Security Research* 1 (2011).

IBM. *An Architectural Blueprint for Autonomic Computing*. Hawthorne, NY: IBM, 2005.

Intel Security. *Net Losses: Estimating the Global Cost of Cybercrime*. Santa Clara, CA: Intel Security Center for Strategic and International Studies 2014.

IPass. "The Global Public Wi-Fi Network Grows to 50 Million Worldwide Wi-Fi Hotspots." January 20, 2015. https://www.ipass.com/press-releases/the-global-public-wi-fi-network-grows-to-50-million-worldwide-wi-fi-hotspots/.

Iasiello, Emilio. "Hacking Back: Not the Right Solution." *Parameters* 44, no. 3 (2014).

James, E. P., M. J. Tudor, S. P. Beeby, N. R. Harris, P. Glynne-Jones, J. N. Ross, and N. M. White. "An Investigation of Self-Powered Systems for Condition Monitoring Applications." *Sensors and Actuators A: Physical* 110, no. 1 (2004).

Jarvis, Lee, Stuart Macdonald, and Andrew Whiting. "Constructing Cyberterrorism as a Security Threat: A Study of International News Media Coverage." *Perspectives on Terrorism* 9, no. 1 (2015).

Juniper Research. "Cybercrime Will Cost Businesses Over $2 Trillion by 2019." May 12, 2015. http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

Kallberg, Jan. "In Cyber, Time is of the Essence." The Cyber Defense Review. January 28, 2016. http://www.cyberdefensereview.org/2016/01/28/in-cyber-time-is-of-the-essence/.

Kerner, Rotem. "Remote Code Execution in CCTV-DVR Affecting over 70 Different Vendors." Kerner on Security. March 22, 2016. http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html.

Klein, John J. "Deterring and Dissuading Cyberterrorism." *Journal of Strategic Security* 8, no. 4 (2015).

Kreidl, O. Patrick, and Tiffany M. Frazier. "Feedback Control Applied to Survivability: A Host-Based Autonomic Defense System." *IEEE transactions on Reliability* 53, no. 1 (2004).

Leed, Maren. Offensive Cyber Capabilities at the Operational Level. Washington, DC: Center for Strategic International Studies, 2013. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf.

Mao, Rui, Honglong Xu, Wenbo Wu, Jianqiang Li, Yan Li, and Minhua Lu. "Overcoming the Challenge of Variety: Big Data Abstraction, the Next Evolution of Data Management for AAL Communication Systems." *IEEE Communications Magazine* 53, no. 1 (2015).

Mazanec, Brian M. "Why International Order in Cyberspace Is Not Inevitable." *Strategic Studies Quarterly* 9, no. 2 (2015).

McConnell, Steve. "Software Quality at Top Speed." SteveMcConnel.com. August 1996. http://www.stevemcconnell.com/articles/art04.htm.

Miercom. *BluVector Cyber Threat Detection and Hunting Program*. East Windsor, NJ: Miercom, 2016.

MITRE. "Cybersecurity: Situational Awareness." Accessed August 8, 2016. https://www.mitre.org/capabilities/cybersecurity/situation-awareness.

———. "Threat-Based Defense: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)." Bedford, MA: MITRE Corporation, 2012.

Muccini, Henry, Mohammad Sharaf, and Danny Weyns. "Self-Adaptation for Cyber-Physical Systems: A Systematic Literature Review." *Proceedings of the 11th International Workshop on Software Engineering for Adaptive and Self-Managing Systems* (2016).

Nakashima, Ellen, and Matt Zapotosky. "U.S. Charges Iran-Linked Hackers with Targeting Banks, N.Y, Dam." *Washington Post*. March 24, 2016. https://www.washingtonpost.com.

National Institute of Standards and Technology. “Cybersecurity Framework Frequently Asked Questions.” Last modified October 21, 2015. http://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics.cfm.

———. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, MD: National Institute of Standards and Technology, 2014.

National Security Agency. “Active Cyber Defense Fact Sheet.” Accessed July 13, 2016. https://www.iad.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm.

———. “Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today’s Highly Networked Environments.” Accessed August 21, 2016. https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf.

Nesmeyanov, E. E., A. M. Rudenko, and V. V. Kotlyarova. “Sociocultural Analysis of Cyberterrorism in Social Nets within the Problems of Information Safety of Russian Society.” *Science Almanaca Black Sea Countries* 4 (2015).

Ng, Andrew. “Machine Learning.” Coursera. Accessed August 28, 2016. https://www.coursera.org/learn/machine-learning.

Nguyen, Cuong M., Jeffrey Mays, Dakota Plesa, Smitha Rao, Minh Nguyen, and J-C. Chiao. “Wireless Sensor Nodes for Environmental Monitoring in Internet of Things.” *2015 IEEE MTT-S International Microwave Symposium*.

Paganini, Pierluigi. “Proofpoint Discovered More Than 750,000 Phishing and SPAM Emails Launched from ‘Thingbots’ Including Televisions, Fridge.” Security Affairs. January 19, 2014. http://securityaffairs.co/wordpress/21397/cyber-crime/iot-cyberattack-large-scale.html.

———. “Speaking at Kaspersky Lab’s Industry Analyst Summit Costin Raiu, Revealed that the Cost for APT Campaign is Dramatically Dropping.” Security Affairs. February 9, 2014. http://securityaffairs.co/wordpress/22056/cyber-crime/apt-cost-dramatically-dropping.html.

Pescatore, John. *Continuous Diagnostics and Mitigation: Making it Work*. Bethesda, MD: SANS Institute, 2014.

Ponemon Institute. *2015 Global Report on the Cost of Cyber Crime*. Traverse City, ME: Ponemon Institute, 2015.

Pratt, Mary K. “As Threats to Data Spread, Security Info Sharing Debate Heats Up.” TechTarget. Accessed August 28, 2016. http://searchcompliance.techtarget.com/feature/As-threats-to-data-spread-security-info-sharing-debate-heats-up.

PricewaterhouseCoopers. “Security Incidents Continue to Rise in Cost and Frequency while Budgets Decrease, According to PwC, CIO and SCO’s The Global State of Information Security Survey 2015.” September 30, 2014. http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html.

———. *Why You Should Adopt the NIST Cybersecurity Framework*. New York: PricewaterhouseCoopers, 2014.

Richards, Jason. “Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security.” *International Affairs Review* 18, no. 2 (2009).

Roth, Siegmar, and David Carroll. *One-Dimensional Metals: Conjugated Polymers, Organic Crystals, Carbon Nanotubes and Graphene*. Hoboken, NJ: John Wiley & Sons, 2015.

Rouse, Margaret, “Autonomic Computing.” WhatIs. Accessed July 13, 2016. http://whatis.techtarget.com/definition/autonomic-computing.

———. “Internet of Things (IoT).” WhatIs. Accessed August 28, 2016. http://internetofthingsagenda.techtarget.com/definition/internet-of-Things-IoT.

Sanger, David E., and Eric Schmitt. “Spy Agency Consensus Grows That Russia Hacked D.N.C.” New York Times. July 26, 2016. http://www.nytimes.com.

Schlachter, Fred. “No Moore’s Law for Batteries.” *Proceedings of the National Academy of Sciences* 110, no. 14 (2013).

Schapire, Rob. “COS 511: Theoretical Machine Learning.” Princeton University, Lecture Notes, February 4, 2008. http://www.cs.princeton.edu/courses/archive/spr08/cos511/scribe_notes/0204.pdf.

Schlein, Ted. “The Five Tough Truths of Cybersecurity.” TechCrunch. May 31, 2014. https://techcrunch.com/2014/05/31/the-five-tough-truths-of-cybersecurity-software/.

Shi, Mayue, Jinxin Zhang, Haotian Chen, Mengdi Han, Smitha A. Shankaregowda, Zongming Su, Bo Meng, Xiaoliang Cheng, and Haixia Zhang. “Self-Powered Analogue Smart Skin.” *ACS Nano* 10, no. 4 (2016).

Small, Prescott E. *Defense in Depth: An Impractical Strategy for a Cyber World*. Bethesda, MD: SANS Institute 2011.

Smith, Aaron. “U.S. Smartphone Use in 2015.” Pew Research Center. April 1, 2015. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

Taylor, Harriet. “Biggest Cybersecurity Threats in 2016.” CNBC. December 28, 2015. http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html.

Timberg, Craig. “Net of Insecurity: A Flaw in the Design.” *Washington Post*. May 30, 2015. http://www.washingtonpost.com/.

Trend Micro. “Researchers Discover a Not-So-Smart Flaw in Smart Toy Bear.” February 4, 2016. http://www.trendmicro.com/vinfo/us/security/news/internet-of-things/researchers-discover-flaw-in-smart-toy-bear.

US-CERT. “Automated Information Sharing (AIS).” Accessed August 27, 2016. https://www.us-cert.gov/ais.

Veeramachaneni, Kalya, Ignacio Arnaldo, Alfredo Cuesta-Infante, Vamsi Korrapati, Costas Bassias, and Ke Li. “AI^2: Training a Big Data Machine to Defend.” Accessed September 17, 2016. https://people.csail.mit.edu/kalyan/AI2_Paper.pdf.

Vollmer, Todd, Milos Manic, and Ondrej Linda. “Autonomic Intelligent Cyber-Sensor to Support Industrial Control Network Awareness.” *IEEE Transactions on Industrial Informatics* 10, no. 2 (2014).

Voris, Jonathan, Jill Jermyn, Nathaniel Boggs, and Salvatore Stolfo. “Fox in the Trap: Thwarting Masqueraders via Automated Decoy Document Deployment.” *Proceedings of the Eighth European Workshop on System Security* (2015).

Zhao, Ziming, Mukund Sankaran, Gail-Joon Ahn, Thomas J. Holt, Yiming Jing, and Hongxin Hu. “Mules, Seals, and Attacking Tools: Analyzing 12 Online Marketplaces.” *IEEE Security & Privacy* 14, no. 3 (2016).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California