NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

21ST CENTURY CRIME: HOW MALICIOUS ARTIFICIAL INTELLIGENCE WILL IMPACT HOMELAND SECURITY

by

Kevin M. Peters

March 2019

Thesis Advisor:	Shannon A. Brown
Second Reader:	Cristiana Matei

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

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

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2019	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE 21ST CENTURY CRIME: HOW MALICIOUS ARTIFICIAL INTELLIGENCE WILL IMPACT HOMELAND SECURITY	5. FUNDING NUMBERS
6. AUTHOR(S) Kevin M. Peters	
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.

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

13. ABSTRACT (maximum 200 words)

Artificial intelligence (AI) is a field of research with the potential to radically change society's use of information technology, particularly how personal information will be interconnected and how private lives will be accessible to cybercriminals. Criminals, motivated by profit, are likely to adapt future AI software systems to their operations, further complicating present-day cybercrime investigations. This thesis examines how transnational criminal organizations and cybercriminals may leverage developing AI technology to conduct more sophisticated criminal activities and what steps the homeland security enterprise should take to prepare. Through a future scenario methodology, four scenarios were developed to project how cybercriminals might use AI systems and what should be done now to protect the United States from the malicious use of AI. This thesis recommends that homeland security officials expand outreach initiatives among private industry and academia that are developing AI systems to understand the dual-use implications of emerging AI technology and to provide public security perspectives to AI research entities. Finally, this thesis recommends that federal agencies develop specific initiatives—aligning with existing national cyber and AI strategies—that confront the potential challenge of future, AI-enabled cybercrime.

14. SUBJECT TERMS transnational organized crime, Darknet, emerging technology, homeland security, artificial intelligence, cybercrime	15. NUMBER OF PAGES 121
	16. PRICE CODE

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

NSN 7540–01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

21ST CENTURY CRIME: HOW MALICIOUS ARTIFICIAL INTELLIGENCE WILL IMPACT HOMELAND SECURITY

Kevin M. Peters
Deputy Director, Current Intelligence, Current & Emerging Threats Center,
Office of Intelligence & Analysis, Department of Homeland Security
BA, University of Maryland University College, 2006
MBA, Pennsylvania State University, 2009

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
March 2019

Approved by: Shannon A. Brown
Advisor

Cristiana Matei
Second Reader

Erik J. Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Artificial intelligence (AI) is a field of research with the potential to radically change society's use of information technology, particularly how personal information will be interconnected and how private lives will be accessible to cybercriminals. Criminals, motivated by profit, are likely to adapt future AI software systems to their operations, further complicating present-day cybercrime investigations. This thesis examines how transnational criminal organizations and cybercriminals may leverage developing AI technology to conduct more sophisticated criminal activities and what steps the homeland security enterprise should take to prepare. Through a future scenario methodology, four scenarios were developed to project how cybercriminals might use AI systems and what should be done now to protect the United States from the malicious use of AI. This thesis recommends that homeland security officials expand outreach initiatives among private industry and academia that are developing AI systems to understand the dual-use implications of emerging AI technology and to provide public security perspectives to AI research entities. Finally, this thesis recommends that federal agencies develop specific initiatives—aligning with existing national cyber and AI strategies—that confront the potential challenge of future, AI-enabled cybercrime.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- A. RESEARCH QUESTION....1
- B. PROBLEM STATEMENT....1
- C. RESEARCH DESIGN....4
  - 1. Instrumentation....4
  - 2. Steps of Analysis....4
  - 3. Intended Output....6
- D. BREAKING DOWN THE SCENARIOS....6
  - 1. Overview of Scenario 1: Autonomous Weapons Systems....8
  - 2. Overview of Scenario 2: Deepfakes....9
  - 3. Overview of Scenario 3: Identity Theft....10
  - 4. Overview of Scenario 4: Virtual Kidnapping....10
- E. CHAPTER SUMMARY....11

II. LITERATURE REVIEW....13
- A. TCOS AND CYBERCRIMINALS, ONLINE ILLICIT MARKETS, AND THEIR ADAPTATION TO NEW TECHNOLOGY....13
- B. ARTIFICIAL INTELLIGENCE: A BOLD NEW AGE OR ARMAGEDDON?....18
- C. TRENDS IN ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND DEEP LEARNING....22
- D. MALICIOUS USE OF ARTIFICIAL INTELLIGENCE SYSTEMS....26
- E. CHAPTER SUMMARY....30

III. SCENARIOS....33
- A. SCENARIO 1: AUTONOMOUS WEAPON SYSTEMS....33
- B. SCENARIO 2: DEEPFAKES....37
- C. SCENARIO 3: IDENTITY THEFT....39
- D. SCENARIO 4: VIRTUAL KIDNAPPING....42
- E. CHAPTER SUMMARY....44

IV. TACTICAL AND OPERATIONAL RESPONSE....47
- A. EDUCATING LAW ENFORCEMENT ON CYBERCRIME AND EMERGING AI TECHNOLOGIES....48
- B. ADAPTING ILP TO THE MALICIOUS AI THREAT....49
- C. ENVIRONMENT OF AI-ENABLED CYBERCRIME....53

D. IDENTIFYING PERPETRATORS OF AI-ENABLED CYBERCRIME 55
E. INTERAGENCY AND INTERNATIONAL PARTNERSHIPS TO INVESTIGATE MALICIOUS AI 57
F. CHAPTER SUMMARY 59

V. STRATEGY AND POLICY CONSIDERATIONS 61
B. U.S. CYBERSECURITY STRATEGIES 62
C. CYBERSECURITY VERSUS CYBERCRIME 64
D. EXAMINING HOW THE UNITED KINGDOM CONFRONTS CYBERCRIME 66
E. EXAMINING HOW FRANCE CONFRONTS CYBERCRIME 68
F. WHAT CAN THE UNITED STATES LEARN FROM THE UK AND FRANCE? 71
G. AUSTRALIA: A POSSIBLE MODEL FOR TRACKING CYBERCRIME 71
H. CHAPTER SUMMARY 74

VI. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS 75
A. INTRODUCTION 75
B. FINDINGS 75
C. CONCLUSIONS 76
D. RECOMMENDATIONS 78
1. Develop Strategies to Combat Malicious AI that Align with the New National Strategy for AI and the National Cybercrime Strategy 78
2. Expand Engagements with Private Industry and Academic Institutions 79
3. Expand Partnerships with International Law Enforcement Organizations to Combat AI-Enabled Cybercrime 80
E. NEXT STEPS FOR FUTURE RESEARCH 81
F. CHAPTER SUMMARY 83

LIST OF REFERENCES 85

INITIAL DISTRIBUTION LIST 99

LIST OF FIGURES

Figure 1. Relationship of Artificial Intelligence, Machine Learning, and Deep Learning 23

Figure 2. Photographs of Jennifer Lawrence and Steve Buscemi (Top) and Deepfake Video Combining Their Images (Bottom).....28

Figure 3. Photograph (Left) and Deepfake Video (Right) of Daisy Ridley 30

Figure 4. Sample Spear Phishing Email 41

Figure 5. The Interrelationship between Transnational Crime, Identity Crime, Cybercrime, and Fraud.....52

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Overview of Future Scenarios 7

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACORN	Australian Cybercrime Online Reporting Network
AEP	Analytic Exchange Program
AI	artificial intelligence
CEO	chief executive officer
DHS	Department of Homeland Security
DL	deep learning
FBI	Federal Bureau of Investigation
INTERPOL	International Crime Police Organization
ISAC	Information Sharing and Analysis Center
ILP	intelligence-led policing
MIT	Massachusetts Institute of Technology
ML	machine learning
NCA	National Crime Agency (UK)
NCSC	National Cyber Security Centre (UK)
OSINT	open-source intelligence
PII	personally identifiable information
TCOs	transnational criminal organizations
UK	United Kingdom

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Artificial intelligence (AI) has the potential to dramatically transform how society interacts with information technology, particularly how personal information will interconnect with the hardware and software systems people use on a daily basis. The combination of developing AI systems and a digitally connected society could transform our culture in a manner not seen since the Industrial Revolution.[1] Experts in the field of AI disagree on the pace at which the technology will develop; however, cognitive computing and machine learning are likely to affect homeland security in the coming years.[2] Criminals, motivated by profit, are likely to adapt future AI software systems to their operations, further complicating present-day cybercrime investigations.[3] If the homeland security enterprise is going to be prepared for the potential malicious usage of AI technology, it must begin to examine how criminal elements may use the technology and what should be done today to ensure it is ready for tomorrow's threat.

This thesis examines how transnational criminal organizations and cybercriminals may leverage developing AI technology to conduct more sophisticated criminal activities and what steps the homeland security enterprise should take to prepare. A byproduct of ongoing research is that criminals may create malevolent AI. Cybercriminals, motivated by profit, may attempt to develop proxy AI systems that mask their involvement, avoid risk, and direct attribution and responsibility.[4] The malicious use of AI could threaten digital security, and machines could become as proficient at hacking and social engineering

---

[1] Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (New York: W.W. Norton & Company, 2016), loc. 90 of 306, Kindle.

[2] Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence*, 1st ed. (New York: Alfred A. Knopf, 2017), 30.

[3] John Markoff, "As Artificial Intelligence Evolves, so Does Its Criminal Potential," *New York Times*, October 23, 2016, https://www.nytimes.com/2016/10/24/technology/artificial-intelligence-evolves-with-its-criminal-potential.html.

[4] Federico Pistono and Roman V. Yampolskiy, "Unethical Research: How to Create a Malevolent Artificial Intelligence" (paper presented at the Ethics for Artificial Intelligence Workshop, New York, NY, July 9–15, 2016), http://arxiv.org/abs/1605.02817.

as human cybercriminals.[5] The ability to detect cybersecurity attacks from malicious AI is predicated on an examination of these technologies and their application to existing criminal patterns and activities. Criminals have long demonstrated that they are early adopters of new technologies, and they will almost certainly incorporate AI into their criminal enterprises.[6]

This thesis applied a red-teaming approach—using a future scenario methodology—to project how cybercriminals may use AI systems and what should be done now to protect the United States from the malicious use of AI. The analysis first considered current fields of AI research, likely timelines for technological developments, and AI's perceived impact on daily life in the United States over the next ten years. Next, the analysis examined how present-day cybercrime threats—such as remote-controlled aerial systems, the ability to create fake video files, spear phishing attacks, and social media profiling—could be enhanced by future AI systems. The final step in the analysis was to examine these scenarios and build countermeasures that homeland security officials in the United States could employ to mitigate the potential risks of malicious AI. The criminal use of AI will likely affect multiple echelons of government, and a strategic review analyzes the policy framework required to confront the threats identified in the AI scenarios. Best practices from foreign partners were examined to find strategies and methodologies that could be applied within the United States. A tactical review analyzed how law enforcement agencies could respond to the attacks in the AI scenarios and what existing law enforcement operations could be adapted to prepare for malicious AI.

The progression of AI is uncertain, and the scenarios highlight the ways that cybercriminals could leverage even relatively minor technological developments. Education and awareness of emerging technologies should form the basis of how cybercrime is examined. The thesis recommends that the homeland security enterprise expand outreach programs and partner with private industry and academia that are

---

[5] Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Oxford: University of Oxford, February 2018), http://arxiv.org/abs/1802.07228.

[6] Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World* (New York: Anchor Books, 2016), loc. 1 of 392, Kindle.

developing AI systems in order to understand the dual-use implications of emerging AI technology. Public security officials also have much to offer the AI research community; perspectives from law enforcement, emergency response, policymakers, and intelligence officials will be vital to assisting in the development of safe and ethical AI systems. Federal agencies with cybercrime enforcement authority should develop strategies that align with existing national cyber and AI strategies and can form the framework for confronting the potential challenge of future AI-enabled cybercrime.

This research concludes that the potential threats posed by cybercriminals' use of AI are not a challenge that can be mitigated by any one agency. Rather, a coalition of willing partners across multiple echelons of government, private industry, and academia will need to work together to combat future cybercrime. International partnerships with law enforcement agencies and associations that support anti-crime operations will also be critical in tracking, investigating, and prosecuting future cybercrime. This thesis begins the discussion of how to confront the challenge of future AI-enabled cybercrime and seeks to expand awareness of how to combat dual-use emerging technologies.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I want to begin by thanking my amazing wife, Andrea, for her ever-present support and for her patience with all of my academic interests. This program has allowed me to return to the city where we first met, retrace our first days together, and remember just how fortunate I was to have found her 24 years ago. To my beautiful daughters, Kelcey and Morgen, thank you for your support and understanding when Daddy needed to study or when I was away. To Lorena Gonzalez Penayo, Katerine Soler, and Natalia Hernandez Munoz, I love you so much. Thank you for always taking such great care of our "terremoticos" while I was away at school.

I am grateful for the support of my entire family and want to extend a special thanks to Dan, Betsy, Colleen, and Erika Gallagher as well as my wonderful grandmother, Beth. I do not think I could have completed my thesis without the quiet time to relax in Half Moon Bay or the peaceful tranquility of the family ranch in Crows Landing. This program afforded me the chance to visit my family and to reconnect with my Californian roots.

I want to thank my advisors, Dr. Shannon Brown and Dr. Cristiana Matei, for their support and counsel. This thesis has been an amazing and challenging journey, and I appreciate their encouragement and guidance. I also want to thank Dr. Lauren Wollman for always being available to answer my calls or respond to my Slack messages during all of my freak-out moments. I am grateful for all the support from the entire CHDS team, and I would like to extend a special thanks to Greta Marlatt for her assistance at multiple stages of my thesis.

To my classmates, I am honored to be a member of the 1705/1706 cohort, and I have enjoyed all our time together throughout the past 18 months. This is an amazing group of homeland security leaders, and I am humbled by the service and contributions of my classmates. I am lucky to be part of this group, and I wish everyone the best in their future endeavors.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> By far the greatest danger of Artificial Intelligence is that people conclude too early that they understand it.
>
> —Eliezer Yudkowsky[1]

A. RESEARCH QUESTION

This thesis answers the following questions: How might transnational criminal organizations (TCOs) and cybercriminals leverage developing AI technology to conduct more sophisticated criminal activities, and how should the homeland security enterprise prepare?[2]

B. PROBLEM STATEMENT

Artificial intelligence (AI) is a field of research that has the potential to radically change society's use of information technology, particularly how personal information will be interconnected and how private lives will be accessible to cybercriminals. Experts in the field of AI disagree on the pace at which the technology will develop; however, cognitive computing and machine learning are likely to affect homeland security in the near future.[3] The potential adaption of commercially available unmanned aerial systems with homemade weapon systems and emerging cognitive computing systems should concern

---

[1] Amnon H. Eden et al., *Singularity Hypotheses: A Scientific and Philosophical Assessment* (New York: Springer, 2012), 183.

[2] "Transnational organized crime refers to those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/ or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. There is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures." National Security Council, "Strategy to Combat Transnational Organized Crime: Definition," Obama White House, accessed August 26, 2018, https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/definition. Cybercrimes are crimes committed on the internet using the computer as either a tool or a targeted victim. Aghastise E. Joseph, "Cybercrime Definition," Computer Crime Research Center, accessed August 26, 2018, http://www.crime-research.org/articles/joseph06/.

[3] Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence*, 1st ed. (New York: Alfred A. Knopf, 2017), 30.

homeland security practitioners and policymakers. The international community is so concerned about the potential development of unmanned weapons systems that some scholars have called for an international treaty banning the creation of autonomous weapons systems, similar to past chemical weapons bans.[4] Some researchers fear that autonomous weapons, designed by any nation, could accidentally cause mass civilian casualties.[5] In the worst-case scenario, the development of autonomous weapons systems could spark a 21st-century arms race similar to the nuclear arms race of the 20th century.[6] Criminals and other non-state actors could leverage existing autonomous aerial drones to build homemade weaponized drones in the United States. The threats posed by homemade, AI enhanced, weaponized aerial systems are likely to be on the nearer end of the development horizon, and homeland security professionals need to pay close attention to the progression of this potential weapons system.

The term artificial intelligence has been generally regarded as a domain of computer science research that includes cognitive computing, machine learning, deep learning, computer vision, natural-language processing, and robotics.[7] Today, AI researchers are drawing parallels with how humans think. A recent definition from Stanford University's 100 Year Study on Artificial Intelligence describes AI as "a science and a set of computational technologies that are inspired by—but typically operate quite differently from—the ways people use their nervous systems and bodies to sense, learn, reason, and take action."[8] Cognitive computing systems develop a coherent, complete, and unified understanding, and these systems are often compared to the human brain's processing

---

[4] Peter Asaro, "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making," *International Review of the Red Cross* 94, no. 886 (June 2012): 687–709, https://doi.org/10.1017/S1816383112000768.

[5] Tegmark, *Life 3.0*.

[6] Tegmark.

[7] Nils J. Nilsson, *Principles of Artificial Intelligence* (Palo Alto: Tioga, 1980), 2.

[8] Peter Stone et al., *Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence* (Stanford: Stanford University, 2016), https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf.

abilities.[9] Cognitive computing has the potential to enhance decision-making, augmentation, connectivity, and the innovation of individuals and organizations.[10]

One byproduct of ongoing research might be that criminals begin to create malevolent AI. Cybercriminals who are motivated by profit might attempt to develop proxy AI systems that mask their involvement, avoid risk, and direct attribution and responsibility.[11] The malicious use of AI could threaten digital security, and machines could become as proficient at hacking and social engineering as human cybercriminals.[12] The ability to detect cybersecurity attacks from malicious AI is predicated on an examination of these technologies and their application to existing criminal patterns and activities. Criminals have long demonstrated that they are early adopters of new technologies.[13]

Homeland security leaders should begin to examine how AI can be used for harm and what steps can be taken to ensure public safety. Given the uncertain future for AI research, implementation, and wide-scale adoption, the development of future scenarios may provide a framework for analyzing potential threats. After examining four scenarios written around challenges posed by more advanced forms of AI, this thesis applies red-teaming processes to anticipate how criminals could leverage technology in future crimes. The combination of future scenarios and red-teaming helps to project how emerging technology may be used for criminal purposes and then to develop proactive measures to mitigate the potential threats the homeland security enterprise is likely to face.

---

[9] Dharmendra S. Modha et al., "Cognitive Computing," *Communications of the ACM* 54, no. 8 (August 2011): 62–71, https://doi.org/10.1145/1978542.1978559.

[10] H. Demirkan, J. C. Spohrer, and J. J. Welser, "Digital Innovation and Strategic Transformation," *IT Professional* 18, no. 6 (2017): 14–18, https://doi.org/10.1109/MITP.2017.3051332.

[11] Federico Pistono and Roman V. Yampolskiy, "Unethical Research: How to Create a Malevolent Artificial Intelligence" (paper presented at the Ethics for Artificial Intelligence Workshop, New York, NY, July 9–15, 2016), http://arxiv.org/abs/1605.02817.

[12] Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Oxford: University of Oxford, February 2018), http://arxiv.org/abs/1802.07228.

[13] Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World* (New York: Anchor Books, 2016), loc. 1 of 392, Kindle.

C. RESEARCH DESIGN

This thesis is principally a projection of how transnational criminal organizations, individual cybercriminals, or other illicit actors who are motivated by profit might use AI and what should be done now to protect the United States from the malicious use of AI. This thesis neither examines how nation-states or non-state organizations might use AI against U.S. interests nor explores the ethical considerations of developing or using AI.[14] This thesis further assumes that AI research will progress despite concerns that its developments will bring negative socio-economic impacts to society. The future scenarios in this study also assume that criminal activities will be driven by profit; future crimes committed for moral, political, or ethical purposes are outside the scope of this research. Finally, this study assumes that AI will be familiar to and widely adopted across all social-economic groups in the United States, thus giving criminals the ability to use malicious AI on a large scale. In AI's likely transition from academic settings and corporate laboratories to a general population that experiments with machine learning, robotics, and additive manufacturing, the technologies will likely fall in the hands of a few dedicated enthusiasts who will hone their skills to produce viable malicious systems in service of TCOs.

1. Instrumentation

The artificial intelligence research in this study relies on peer-reviewed journals, published findings from private industry, academic conference presentations, and open-source news reporting that informs the general public on advances in AI. This inquiry into TCO activities and how they could be adapted to future AI breakthroughs is supported by peer-reviewed, criminal justice journals, the published accounts of cybercriminals, researchers in the field of cryptocurrencies, and case studies of Dark Net criminal activities.

2. Steps of Analysis

The analysis outlined in this thesis follows several steps to explain the potential trajectories of AI research, the ways criminal actors could leverage AI against the United States, and the steps the homeland security enterprise should be taking now to protect

[14] Tegmark, *Life 3.0*, 126.

society from malicious AI. First, the analysis considered current fields of AI research, likely timelines for technologic developments, and the projected impact of AI in daily life in the United States over the next 10 years. This step considered multiple viewpoints on AI development and favored the most accelerated projections for AI development timelines. This thesis uses scenario planning, future studies, and red-teaming methods to develop four scenarios whereby future AI developments dramatically change significant aspects of society.[15] The first scenario examines how a criminal could build fully autonomous weapons systems from commercially available components and how the systems could be designed to minimize the criminal's exposure to detection. The second scenario explores how future AI technology could create deepfake video files that appear to be genuine footage for the purpose of extorting victims. The third scenario demonstrates how cybercriminals could create a malicious AI interface that fools a person into divulging personal information or giving access to sensitive data. Finally, the fourth scenario explores how AI systems could convince someone that a loved one has been virtually kidnapped for purposes of ransom.

After developing the four future AI scenarios, the second step was to consider how AI could be used for malicious purposes. This thesis uses scenario planning to explore, from a red-team perspective, how AI technology might be used against the United States by criminal actors. Scenario planning facilitates foresight and helps to identify potential outcomes that may seem unthinkable.[16] Scenario planning can also form the basis for decision-making and future strategic development efforts.[17] The first scenario shows how criminal actors could build an autonomous weapon system and use it to conduct a financially motivated assassination of a public official. The second scenario demonstrates how a deepfake video could compromise a person's reputation and be used to extort financial interests. The third scenario shows how AI can enhance current spearphishing

---

[15] A. J. Masys, "Black Swans to Grey Swans: Revealing the Uncertainty," *Disaster Prevention and Management* 21, no. 3 (2012): 320–35, https://doi.org/10.1108/09653561211234507.

[16] Masys, 322.

[17] Bill Ralston and Ian Wilson, *The Scenario-Planning Handbook: A Practitioner's Guide to Developing and Using Scenarios to Direct Strategy in Today's Uncertain Times* (Mason, OH: Thomson/South-Western, 2006), 21.

tactics and make detection extremely difficult. The last scenario shows how AI could leverage information from a victim's social media accounts and online activity to generate a realistic pattern-of-life profile to commit a virtual kidnapping.

The third and final step in the analysis was to examine these scenarios and build countermeasures that homeland security officials in the United States could employ to mitigate the potential risks of malicious AI. The criminal use of AI will likely affect multiple echelons of government. A strategic review analyzes the policy framework required to confront the threats identified in the AI scenarios. A tactical review analyzes how to respond to the attacks in the AI scenarios. Last, a technical review outlines recommendations for homeland security officials that will promote awareness among the community of how criminals could use emerging AI technology.

3. Intended Output

The intended output of this research is twofold: a clearer (if hypothetical) sense of how AI could be used by criminals motivated by profit and policy recommendations for proactively protecting against the unintended consequences of AI research, development, and implementation. The intended audience for this thesis includes federal, state, and local law enforcement, as well as federal, state, and local agencies with homeland security responsibilities.

D. BREAKING DOWN THE SCENARIOS

The four future scenarios underscore the complexities that malicious AI will bring to the homeland security environment, and they also demonstrate how the modern information environment will merge with developing AI. Emerging technologies beyond AI will interconnect in new ways and—with information systems and the amount of information that will be available for deep-learning algorithms—expand exponentially.[18] Personally identifiable information (PII) and society's use of social media platforms will

[18] P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Books, 2010), 96.

also connect us in new ways and offer AI developers new information sources for building more complex deep-learning tools.[19]

Table 1 highlights how the four future scenarios interrelate with a range of themes discussed throughout this thesis. Each of the fictitious criminal actors relies on a variety of societal and geopolitical realities to enable the use of malicious AI in their activities. Several areas, specifically international relations, virtual borders, social media, and machine learning (ML) technologies, are used in all four future scenarios. The table seems to suggest that the homeland security enterprise has to understand the environment in which malicious AI could be deployed to develop policies and strategies to protect against new cybercrime threats.

Table 1. Overview of Future Scenarios

	Scenario 1 Autonomous Weapon Systems	Scenario 2 Deep Fakes	Scenario 3 Identity Theft	Scenario 4 Virtual Kidnapping
Personally Identifiable Information				
International Relations				
Virtual Borders				
Online Illicit Markets				
Emerging Technology				
Social Media				
Machine Learning				
Deep Learning				

AI systems, particularly ML systems, presently being developed use large amounts of data to keep improving performance, without human intervention.[20] As data are

[19] William D. Eggers, *Delivering on Digital: The Innovators and Technologies That Are Transforming Government* (New York: Rosetta Books, 2016), loc. 3791 of 4730, Kindle.

[20] Erik Brynjolfsson and Andrew McAfee, "The Business of Artificial Intelligence: What It Can—and Cannot—Do for Your Organization," *Harvard Business Review*, July 2017, 3–11.

processed by ML tools, neural networks analyze the information and produce sophisticated models that can classify even larger datasets.[21] Cybercriminals could use ML neural networks to process large amounts of information and build target profiles of potential victims. PII—information that can be used to distinguish or trace an individual's identity—that has been stolen and sold on the Dark Net and the social media activity of average users offer malicious AI systems a treasure trove of data to be used in criminal activities.[22] Further complicating matters, emerging technologies and consumer products are becoming increasingly connected to the Internet, thereby unlocking new data sources from which AI systems can learn. Malicious AI will connect with a wide range of technologies and have the ability to learn from daily, interconnected activities.

1. Overview of Scenario 1: Autonomous Weapons Systems

In the first scenario, a Chinese graduate school student constructs an autonomous weapon system that is capable of independently searching, acquiring, and conducting an assassination at a public event. Although terrorism and politically motivated crimes are outside the scope of this thesis, this attack vector is financially motivated and targets a public official for assassination due to his presence on a Dark Net assassination market. A central aspect of this scenario is the attacker's ability to combine AI with commercial drone technology to create an autonomous weapons system capable of conducting an attack without direct human guidance. The attacker, as shown in the other scenarios, travels internationally during the attack phase, which complicates law enforcement efforts to investigate the malicious AI-enabled crime.

Scenario 1 references current research on autonomous weapons systems and illicit online markets to anticipate a future threat that the homeland security enterprise may encounter. Paul Scharre and P. W. Singer are two notable researchers who have examined

---

[21] Bernard Marr, "What Is the Difference between Deep Learning, Machine Learning and AI?," *Forbes*, December 8, 2016, https://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference-between-deep-learning-machine-learning-and-ai/#181f5b7426cf.

[22] Clay Johnson III, "Safeguarding against and Responding to the Breach of Personally Identifiable Information," OMB Memorandum M-07-16 (Washington, DC: Office of Management and Budget, May 22, 2007), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf.

the future of automated systems in combat, and their research has framed and forecasted a possible scenario for an armed drone attack within the United States.[23] Jamie Bartlett and James Martin have researched online illicit markets beyond illicit narcotics sales, and their analysis of assassination markets show how criminals could profit from an attack carried out on a particular date.[24] Although this scenario may seem unrealistic today, distinct elements are presently challenging homeland security officials, and commercially available drones have been weaponized. Researchers at the Naval Postgraduate School have developed and tested software that allows aerial drones to conduct combat operations autonomously.[25] Although there have been limited discoveries of assassination markets on the deep web, online contract killings have been attempted. When Silk Road mastermind Ross Ulbricht—known also as the Dread Pirate Roberts—was arrested by the Federal Bureau of Investigation (FBI), he had attempted to contract a killing via an online chat room.[26] The combination of emerging drone technology with autonomous control software could offer would-be assassins the delivery system for future crimes.

2. Overview of Scenario 2: Deepfakes

In the second scenario, a Croatian cyber-criminal creates a deepfake video to extort a successful American businessman. Although deepfakes are becoming more of a present-day challenge, this scenario shows how an internationally based criminal could target a U.S.-based victim and potentially avoid American law enforcement. The cyber-criminal in this scenario conducts his ransom attack and then travels extensively throughout Southeast Asia in an effort to avoid law enforcement detection. The attacker in this scenario also uses

---

[23] Andy Hines, "Strategic Foresight: The State of the Art," *Futurist* 40, no. 5 (October 2006): 18–21, https://www.questia.com/magazine/1G1-150978061/strategic-foresight-the-state-of-the-art.

[24] Jamie Bartlett, *The Dark Net: Inside the Digital Underworld* (Brooklyn: Melville House, 2015), Kindle; and James Martin, "Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket,'" *Criminology & Criminal Justice* 14, no. 3 (July 2014): 351–67, https://doi.org/10.1177/1748895813505234.

[25] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, 1st ed. (New York: W. W. Norton & Company, 2018), 11–12.

[26] Nick Bilton, *American Kingpin: The Epic Hunt for the Criminal Mastermind behind the Silk Road* (New York: Portfolio/Penguin, 2017).

ML technologies, publicly available videos, and PII of the victim to conduct his ransom scheme.

Scenario 2 uses current research into deepfake technologies to examine previous extortion schemes wherein deepfake videos were used. To date, many celebrities have been targeted by deepfake videos that have combined their images with pornographic materials, and foreign governments have attempted to influence French elections with false videos.[27] Deepfake videos are a present-day concern that will only become more challenging as ML technologies develop, increasing the authentic feel of the videos and making detection more difficult.

3. Overview of Scenario 3: Identity Theft

In the third scenario, a criminal hacker uses AI technologies to build sophisticated spear-phishing attacks for the purpose of stealing the identity of victims with valuable information residing in the United States. The hacker also uses deep-learning (DL) tools to quickly search for information on the victims' computers that would be valuable on the Dark Net. This future scenario is based on present-day spear-phishing attacks that are profit-motivated. Additionally, the attacker in this scenario travels extensively throughout Europe while he mines the information he has stolen, making his detection and capture more difficult for partner law enforcement agencies.

Scenario 3 uses research on phishing and spear-phishing attacks to project how these attack vectors can become more sophisticated with the use of future AI technologies. The scenario also highlights how the information that is freely posted online and on social media sites could be used against victims.

4. Overview of Scenario 4: Virtual Kidnapping

In the fourth scenario, a U.S.-based cyber-criminal travels to Costa Rica to research and build sophisticated targeting profiles for the purposes of virtually kidnapping his

[27] Danielle Citron and Robert Chesney, "Deepfakes and the New Disinformation War," *Foreign Affairs*, February 2019, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

victims. The attacker chooses Costa Rica as the location to conduct his planning and attack due to the high volume of tourism from the United States—from which the attacker can hide his criminal activities. The attacker pretends to be a Mexico-based drug cartel, and he sends threatening emails to his targets' families, claiming they will be kidnapped if a ransom is not paid. Although the attacker lacks the ability to actually harm his victims, the profiles and patterns of life he has developed on his targets provide convincing evidence to the families that their children are in danger if the ransom is not paid.

Scenario 4 uses research on recent virtual kidnappings, many of which occur in Mexico, to extrapolate how the threat could evolve with the use of malicious AI. Similar to previous scenarios, PII and social media activity of the potential victims provide the basis for ML and DL technologies to build more sophisticated attack approaches. The attacker in this scenario conducts all of his research in Latin America while on vacation, attempting to avoid detection by U.S. authorities.

E. CHAPTER SUMMARY

The four scenarios examine current criminal threats to imagine how they will evolve when cyber-criminals incorporate emerging AI technologies into their activities. These scenarios challenge policymakers to develop effective strategies for framing the responsibilities of federal, state, and local agencies in combatting future cyber-crime. The homeland security enterprise will also likely need to seek new and broader partnerships with private industry and leading AI research institutions to understand the trajectory of malicious AI threats. International partnerships will be critical to confronting the threats envisioned in the four scenarios, and the homeland security enterprise should explore pathways for collaborating on AI-enabled crimes. Finally, the scenarios demonstrate that the amount of publicly available information and the interconnected nature of society are making us vulnerable to more sophisticated criminal threats. We should examine how our information is being used and what responsibility social media firms bear when their platforms are used for cybercrime.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

If a machine is expected to be infallible, it cannot also be intelligent.

—Alan Turing[28]

The purpose of this chapter is to provide an overview of the scholarly debates on four main themes of research: TCOs and cybercriminals, online illicit markets, and their adaptation to new technologies; AI and perspectives on its utopian or dystopian outcomes; Trends in AI research, machine learning, and decision support systems; and the malicious use of AI systems. These four themes underlie the conditions by which the future use of AI will likely progress, and they form the basis for developing future scenarios in Chapter III. TCOs and cybercriminals will ultimately be the threat actors who use developing AI systems, so examining how they presently adapt to emerging technologies is relevant for projecting their future criminal activities. Projections about the future of AI ranges widely from a spectrum of a utopian future and new renaissance to a dystopian future where autonomous computer systems annihilate the human race. An examination of research into AI systems, machine learning, and deep-learning technology allows for projections of how these technologies will progress in the coming years. Finally, a review of research on how AI systems could be used for malicious purposes illuminates the potential threats that the AI research community believes are on the horizon.

A. TCOS AND CYBERCRIMINALS, ONLINE ILLICIT MARKETS, AND THEIR ADAPTATION TO NEW TECHNOLOGY

The purpose of this literature review is to examine the most relevant research on how criminals use the Dark Net to conduct illegal activities and how these activities are likely to increase in the coming years. TCOs use online illicit markets to traffic a wide range of illegal commodities including humans, narcotics, stolen goods, weapons, PII, and

[28] Alan M. Turing, "Lecture to the London Mathematical Society," Turing Digital Archive, February 20, 1947, http://www.turingarchive.org/viewer/?id=455&title=1.

intellectual property.[29] As AI software develops, legally and illegally developed algorithms are likely to be sold on online illicit markets. It is important that the homeland security enterprise understands how criminals leverage online illicit markets in order to anticipate how AI and cognitive-computing tools will likely be sold in the future.

Several journal articles or reports attempt to measure the volume and scale of sellers engaged in illicit activity on the Dark Net. Silk Road, the illicit drug market that was taken down in 2012, is examined in articles by Nicolas Christian, Marie-Helen Marias, James Martin, and Persi Paoli et al. as a case study of an illicit market operating online.[30] While these articles are foundational, they demonstrate the challenges in measuring illegal activities on the Dark Net. Scholars disagree about the size and scale of online illicit markets, and several researchers have tried different approaches to address this issue. Persi Paoli et al. attempted to measure a short period, a sampling of only six days, of a cryptomarket for weapons trafficking while Nicolas Christian measured eight months of data of online traffic on the Silk Road site for his analysis.[31] Persi Paoli and his colleagues acknowledge that their findings are limited to weapons trafficking markets, which they estimate comprise a small segment of commodities sold on the Dark Net.[32] Christian's analysis focuses on the larger segment of illegal sales on the Dark Net, and he concludes that most online sellers in his research were active only for a few weeks.[33] The results of both articles are potentially combinable because they examine separate segments of illegal markets. However, the results of Persi Paoli et al. need to be validated by more research, given their limited sample.

---

[29] Bartlett, *The Dark Net*, loc. 5 of 310.

[30] Nicolas Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," in *Proceedings of the 22nd International Conference on the World Wide Web* (New York: ACM, 2013), 213–224, https://doi.org/10.1145/2488388.2488408; Marie-Helen Maras, "Inside Darknet: The Takedown of Silk Road," *Criminal Justice Matters* 98, no. 1 (October 2, 2014): 22–23, https://doi.org/10.1080/09627251.2014.984541; Martin, "Lost on the Silk Road," 351–67; and Giacomo Persi Paoli et al., *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, CA: RAND Corporation, 2017), 26–29, https://www.rand.org/pubs/research_reports/RR2091.html.

[31] Persi Paoli et al., *Behind the Curtain*, 26–29; and Christin, "Traveling the Silk Road," 213–224.

[32] Persi Paoli et al., *Behind the Curtain*, 16.

[33] Christin, "Traveling the Silk Road," 10.

James Martin, senior lecturer at Macquarie University in Australia, who studies crime on the Dark Net, used a different methodology to measure online traffic on the Silk Road by examining website postings and message board activities.[34] Martin's analysis focuses on the law enforcement strategy to combat online markets, and he demonstrates how message board postings can tip law enforcement to the potential scale of an online trafficker's operations.[35] Martin's reliance on qualitative observations of illicit markets is significant for law enforcement officials because his recommendations can be used widely for investigations. However, Martin's conclusions are less useful for research purposes because he does not provide a methodology that can be duplicated for more quantitative research.

Rachael Heath-Ferguson, a sociologist at Princeton University, examines some of the work done by the aforementioned researchers in her 2017 journal article about methods for analyzing and measuring illegal activities on the Dark Net.[36] In her research, Heath-Ferguson contends that online scrapping tools used to examine the Silk Road are problematic due to technical shortcomings of the software applications. She claims that mixed research approaches may be more useful, and she recommends analyzing web postings—as Martin does—as a better approach for mixing data collected from quantitative and qualitative methods.

The research into the scale of online illicit markets may be insufficient, and scholars debate how much illegal activity occurs on the Dark Net. Studies of the Silk Road comprise much of this research, and the findings may be too old to be applied to current online illicit markets.[37] The size and scale of current online illicit markets may be a gap that requires more research.

---

[34] Martin, "Lost on the Silk Road," 351–67.

[35] Martin, 364–366.

[36] Rachael Heath-Ferguson, "Offline 'Stranger' and Online Lurker: Methods for an Ethnography of Illicit Transactions on the Darknet," *Qualitative Research* 17, no. 6 (2017): 687–689, https://doi.org/10.1177/1468794117718894.

[37] Maras, "Inside Darknet," 22–23.

Another aspect of this research centers on how online criminals interact with each other on the Dark Net and whether there are established cultural norms for their criminal activities. In this area, several former hackers have written biographies on the criminal culture of the Dark Net. These books are marketed to the general public and provide entertaining stories of criminal exploits, which are of limited research value.[38] Apart from these books, Robert Gehl argues the Dark Net has created a unique environment for political advocacy and a forum for social responsibility.[39] Gehl, a scholar who studies communications, social media, and cultural studies, has interviewed Dark Net forum users to understand their motivations for accessing illicit sites. He believes criminal activity on the Dark Net is but a subset of a broader, positive environment that provides a pathway for people to communicate securely.[40] Gehl describes the Dark Net as a location that offers users "radical freedom of speech" and a forum for dissidents and oppressed populations to communicate.[41]

Gehl's research is significant because his approach offers a different perspective from the other researchers mentioned in this review. While the other researchers are scholars who study criminal justice topics, Gehl has researched how the Dark Net can provide new communication pathways beyond existing social media services like Facebook. Gehl has researched Dark Net forums and message boards by actively engaging with web users. Gehl uses a pseudonym in his research, a practice that Barratt and Maddox rebuke in their ethnology of Dark Net forums.[42] In their research, Monica Barratt and Alexia Maddox—researchers at the National Drug Research Institute at Curtin University

---

[38] Kevin D. Mitnick and William L. Simon, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, 1st ed. (New York: Little, Brown and Company, 2011), 20–32; Kevin Poulsen and Eric Michael Summerer, *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground* (New York, Crown Publishing, 2015), 32–40; and Bartlett, *The Dark Net*, loc. 5–17.

[39] Robert W. Gehl, "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network," *New Media & Society* 18, no. 7 (August 2016): 1219–35, https://doi.org/10.1177/1461444814554900.

[40] Gehl, "Power/Freedom on the Dark Web," 1220; and "About Robert W. Gehl," Webpage of Robert W. Gehl, accessed March 7, 2019, http://www.robertwgehl.org/index.php?styleSheetSelection=mobile.

[41] Gehl, "Power/Freedom on the Dark Web," 1219–35.

[42] Monica J. Barratt and Alexia Maddox, "Active Engagement with Stigmatised Communities through Digital Ethnography," *Qualitative Research* 16, no. 6 (December 2016): 701–19, https://doi.org/10.1177/1468794116648766.

in Australia—use their real identities when engaging on the Dark Net because they believe that the research subjects will be more forthcoming. Their research is focused more broadly on stigmatized communities, and they use the Dark Net and online drug markets as a case study.

The research discussed in this sub-literature section on online illicit markets is generally in agreement regarding the challenges of quantifying criminal activities on the Dark Net. Illegal transactions on the Dark Net and the technology that facilitates criminal activities will continue to be difficult to measure because criminals are able to react to law enforcement tactics and avoid many forms of detection. However, this literature forms a solid baseline of how illegal online markets function, how criminals likely operate, and what the enduring detection and monitoring challenges have been. In the future, cybercriminals will almost certainly leverage online illicit markets in their criminal activities. However, AI and machine learning may offer advantages for tracking illegal activity online, and the homeland security enterprise may want to explore how emerging technologies help close the gap in the understanding of online illicit market activities.

There are several other research areas—beyond the four themes in this literature review—that may provide valuable insights into how malicious AI could affect homeland security in the future. The threat of malicious AI is not limited to the United States, and a study of how foreign partners are confronting cybercrime and AI development is worthy of review. AI research today is confronting the ethical implications of developing artificial general intelligence, and homeland security practitioners should be involved in discussions of machine ethics.[43] Finally, AI has the potential to link personal information in ways yet to be anticipated, and the impact of AI research is an important topic to explore.

[43] Miles Brundage, "Limitations and Risks of Machine Ethics," *Journal of Experimental & Theoretical Artificial Intelligence* 26, no. 3 (September 2014): 355–72, https://doi.org/10.1080/0952813X.2014.895108.

B. ARTIFICIAL INTELLIGENCE: A BOLD NEW AGE OR ARMAGEDDON?

For decades, science fiction has shaped perceptions of how artificial intelligence will evolve and influence future existence. Some authors portray this future as a utopian existence wherein AI will quickly and efficiently respond to every human need. Other authors depict a dystopian future wherein AI will become self-aware and ultimately determine that the human race is a threat that needs elimination. Future AI systems could resemble Isaac Asimov's friendly "Sonny" who ultimately wanted to explore his existence while upholding the Three Laws of Robotics.[44] AI systems could also take a darker, deadlier future course with Terminator robots using advanced machine-learning algorithms to study every aspect of our lives to better exterminate the human race.[45] Science fiction has led to science fact and, at a minimum, helped shape our foundational biases when we explore the possibilities of future AI applications.

Extensive academic research supports the utopian view of future AI, and much of this research promotes the idea that AI will unleash a new age of innovation. Hadley Reynolds and Sue Feldman, co-founders of the Cognitive Computing Consortium, have examined how cognitive computing will fundamentally—and positively—change how we interact with our digital environment.[46] Their research group has attempted to make context computable and to build cognitive computing systems that can adapt and interact with a range of information.[47] Erik Brynjolfsson and Andrew McAfee, two researchers at the Massachusetts Institute of Technology (MIT)'s Center for Digital Business, take a generally positive view of the future of AI although they do highlight how business

---

[44] Isaac Asimov, *Foundation; Foundation and Empire; Second Foundation; The Stars, Like Dust; The Naked Sun; I, Robot* (Minneapolis: Amaranth Press, 1986).

[45] Randall Frakes and William Wisher, *The Terminator* (New York: Bantam Books, 1985).

[46] Hadley Reynolds and Sue Feldman, "Cognitive Computing: Beyond the Hype," *KM World* 23, no. 7 (July/August 2014): 1, 22, http://www.kmworld.com/Articles/News/News-Analysis/Cognitive-computing-Beyond-the-hype-97685.aspx.

[47] Susan Feldman and Hadley Reynolds, "Cognitive Computing: A Definition and Some Thoughts," *KM World* 23, no. 10 (November/December 2014), http://www.kmworld.com/Articles/News/News-Analysis/Cognitive-computing-A-definition-and-some-thoughts-99956.aspx.

dynamics will present challenges in future labor markets.[48] They offer examples of how emerging technology will reshape how industries function, for instance, Airbnb and Uber are hotel and transportation companies, respectively, but do not own hotels or taxis.[49] In their book, Brynjolfsson and McAfee argue that despite the radical changes as a result of emerging technology, such as AI, there are opportunities for adapting industries and society to make the most of the technological advancements.[50] Aguilar et al. also believe that artificial and biological life will merge and that artificial intelligence should be considered another form of life to be studied.[51]

In contrast, a wide body of academic research and magazine articles contends artificial intelligence will ultimately terminate human existence. James Barrat, a researcher and documentary filmmaker, believes that artificial intelligence research is fundamentally dangerous and that AI will eventually develop a sense of self-preservation, which will prove dangerous to humans.[52] Although Barrat's book has been popular among the general population, his analysis is fundamentally flawed as he approaches his research from the position that AI is dangerous technology.[53] Basarab Nicolescu believes that artificial intelligence will achieve a technological singularity whereby it develops to the point that it is capable of autonomous self-improvement, and its objectives are destructive to the human race.[54] Nick Bolstrom, a University of Oxford Philosopher, believes that AI will

---

[48] Amy Bernstein and Anand Raman, "The Great Decoupling: An Interview with Erik Brynjolfsson and Andrew McAfee," *Harvard Business Review*, June 2015, https://hbr.org/2015/06/the-great-decoupling.

[49] Andrew McAfee and Erik Brynjolfsson, *Machine, Platform, Crowd: Harnessing Our Digital Future* (New York: W.W. Norton & Company, 2017), loc. 14 of 404, Kindle.

[50] Brynjolfsson and McAfee, *The Second Machine Age*, 206–218.

[51] Wendy Aguilar et al., "The Past, Present, and Future of Artificial Life," *Frontiers in Robotics and AI* 1 (2014), https://doi.org/10.3389/frobt.2014.00008.

[52] James Barrat, *Our Final Invention: Artificial Intelligence and the End of the Human Era* (New York: Thomas Dunne Books, 2013).

[53] Gary Marcus, "Why We Should Think about the Threat of Artificial Intelligence," *New Yorker*, October 24, 2013, https://www.newyorker.com/tech/elements/why-we-should-think-about-the-threat-of-artificial-intelligence.

[54] Basarab Nicolescu, "The Dark Side of Technological Singularity: New Barbarism," *Cybernetics & Human Knowing* 23, no. 4 (2016): 77–81, http://chkjournal.com/node/237.

ultimately become an existential threat to humanity, and society must prepare now to control a future super-intelligent agent.[55]

In between the two extremes of utopian and dystopian futures for AI is a large group of computer scientists, ethicists, political advocates, and futurists who believe that the future for AI is unclear but now is the time to focus on ethics and goal orientation for all AI research. Max Tegmark, an MIT physics professor, believes that AI is generally a positive scientific development, and the world must focus on developing ethical systems with goals that align with humanity's best interests.[56] His book, *Life 3.0: Being Human in the Age of Artificial Intelligence*, is widely available in many commercial bookstores and was listed as one of President Obama's favorite books in 2018.[57] Tegmark also helped found the Future of Life Institute, which supports research into safeguarding AI development. In 2017, the Future of Life Institute hosted a conference in Pacific Grove, California, developing the 23 Asilomar Principals for the safe and ethical development of beneficial AI technology.[58] In addition to providing an ethical framework for AI research, the Asilomar Principals have also influenced public policy legislation, and in October 2017, the California Senate endorsed the principals.[59] Garry Kasparov, the chess grandmaster who famously lost to IBM's Deep Blue AI chess program in 1997, believes that future AI will help humans make better decisions.[60] In his book, Kasparov outlines his personal journey to the conclusion that AI-enhanced decision-making will unleash a new

---

[55] Grady Booch, "I, for One, Welcome Our New Computer Overlords," *IEEE Software* 32, no. 6 (November 2015): 8–10, https://doi.org/10.1109/MS.2015.134.

[56] Tegmark, *Life 3.0*.

[57] Christina Caron, "Barack Obama's Favorite Book of 2018 Was 'Becoming.' Here's What Else He Liked," *New York Times*, December 31, 2018, https://www.nytimes.com/2018/12/28/arts/obama-favorites-2018.html.

[58] Lisa Morgan, "How to Achieve Ethical Design," *Software Development Times*, November 5, 2018, https://sdtimes.com/ai/how-to-achieve-ethical-design/.

[59] Ani Gevorkian and Jadzia Pierce, "IoT and AI Update: California Legislature Passes Bills on Internet of Things, Artificial Intelligence, and Chatbots," *National Law Review*, October 4, 2018, https://www.natlawreview.com/article/iot-and-ai-update-california-legislature-passes-bills-internet-things-artificial.

[60] Steve Ranger, "Garry Kasparov Is Surprisingly Upbeat about Our Future AI Overlords," ZDNet, November 26, 2018, https://www.zdnet.com/article/garry-kasparov-is-surprisingly-upbeat-about-our-future-ai-overlords/.

and more efficient age.[61] Futurist Richard Yonck also believes that AI will have the ability to connect with humans in deep, emotional ways, and there will be great potential for AI-enabled technology to make us happier and feel more fulfilled.[62] However, Yonck believes, as does Tegmark, that goal orientation is a vital consideration in any AI programming, and the best strategies for successful AI development must include humans.[63]

Both utopian and dystopian viewpoints often agree that at some future time, AI will achieve a singularity wherein computer programming will be able to improve itself without human involvement and ultimately become smarter than humans.[64] However, there is less agreement when it comes to predicting when the singularity will occur. Ray Kurzweil, futurist and Google's director of engineering, believes that AI will pass the Turing test by 2029 and that singularity will occur by 2045.[65] Louis Rosenberg, the CEO of Unanimous AI and an artificial intelligence researcher, believes that singularity will occur closer to 2030.[66] Jurgen Schmidhuber—often referred to in AI research communities as the father of artificial intelligence—also believes that singularity will happen in about 30 years because human/computer interface technology will advance to the point of artificial superintelligence.[67]

Tegmark believes that the timeline for artificial general intelligence, or singularity, is difficult to determine; however, researchers should focus on goal alignment to build

---

[61] Garry Kasparov and Mig Greengard, *Deep Thinking: Where Machine Intelligence Ends and Human Creativity Begins*, 1st ed. (New York: Public Affairs, 2017).

[62] Richard Yonck, *Heart of the Machine: Our Future in a World of Artificial Emotional Intelligence* (New York: Arcade Publishing, 2017).

[63] Ray Kurzweil, "Ray Kurzweil on How We'll End up Merging with Our Technology," *New York Times*, March 14, 2017, https://www.nytimes.com/2017/03/14/books/review/thinking-machines-luke-dormehl.html.

[64] Eden et al., *Singularity Hypotheses*, 2.

[65] Christianna Reedy, "Kurzweil Claims That the Singularity Will Happen by 2045," Futurism, October 5, 2017, https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045.

[66] Jolene Creighton, "The 'Father of Artificial Intelligence' Says Singularity Is 30 Years Away," Futurism, February 14, 2018, https://futurism.com/father-artificial-intelligence-singularity-decades-away.

[67] Creighton.

beneficial AI technologies.[68] In Tegmark's estimation, goal alignment and the development of AI that adheres to moral and ethical frameworks are crucial and need to be a priority for the AI research community today.[69] Tegmark's position—that researchers must be aware of the ethical implications of their research—is vital in examining how cybercriminals may use future AI in their criminal endeavors.

C. TRENDS IN ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND DEEP LEARNING

The AI research community disagrees on a timeline for groundbreaking achievements in AI technology that will radically transform society. In order to examine trends in AI research and its fields, which will ultimately determine the timelines for significant breakthroughs, it is important to dissect the debates surrounding machine learning and deep learning. Although there is debate over the speed at which AI research will progress, Figure 1 depicts the generally accepted hierarchy of AI systems and their interrelation.

---

[68] Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence*, 1st ed. (New York: Alfred A. Knopf, 2017), loc. 659 of 6414, Kindle.

[69] Andrew Anthony, "Max Tegmark: 'Machines Taking Control Doesn't Have to Be a Bad Thing,'" *Observer*, September 16, 2017, https://www.theguardian.com/technology/2017/sep/16/ai-will-superintelligent-computers-replace-us-robots-max-tegmark-life-3-0.

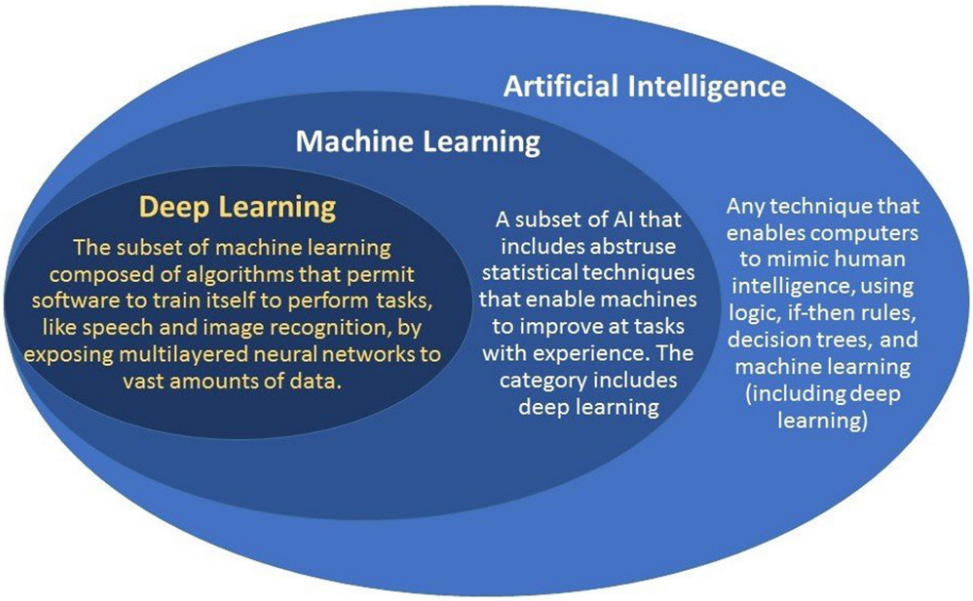

Figure 1. Relationship of Artificial Intelligence, Machine Learning, and Deep Learning[70]

Researchers agree that artificial intelligence is an umbrella term to describe a subfield of computer science that examines how computers can imitate human intelligence.[71] The subfields and terminology of machine learning and deep learning are often intermingled, and there are varying positions on how the fields interrelate. Miles Brundage et al. define machine learning as the ability of machines to access large amounts of data and improve themselves without human intervention and, over time, through experience.[72] Tim Jones generally agrees with this classification of ML although Jones believes that ML also covers research techniques including human supervision.[73] Bernard Marr also believes that machine-learning systems should be categorized as systems that

[70] Source: Meenal Dhande, "What Is the Difference between AI, Machine Learning and Deep Learning?," *Geospatial World* (blog), May 6, 2017, https://www.geospatialworld.net/blogs/difference-between-ai%EF%BB%BF-machine-learning-and-deep-learning/.

[71] Bernard Marr, "The Key Definitions of Artificial Intelligence (AI) That Explain Its Importance," *Forbes*, February 14, 2018, https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#6b85868e4f5d.

[72] Brundage et al., *The Malicious Use of Artificial Intelligence*.

[73] M. Tim Jones, "A Beginner's Guide to Artificial Intelligence, Machine Learning, and Cognitive Computing," *IBM Developer*, June 2, 2017, https://developer.ibm.com/articles/cc-beginner-guide-machine-learning-ai-cognitive/.

use neural networks to classify information in the ways humans do while leveraging increased processing speeds and accuracy.[74] Marr also describes deep learning as a subset of machine learning that more narrowly focuses on tools and techniques as well as methods for solving problems that require thought.[75] Marr describes deep-learning networks as processes that analyze large amounts of data and then classify them accordingly.[76] Janine Sneed agrees with Brundage et al.; however, she disagrees with Marr on the distinction of DL. Sneed agrees that DL is a subset of ML that includes supervised or unsupervised learning, but she believes that DL is identified by artificial neural networks, inspired by the human understanding of biology.[77] Sneed believes that the *deep* in DL is due to the depth of layers that make up artificial neural networks.[78]

A wide body of research focuses on human vis-à-vis machine contests as harbingers of how AI will affect society and the potential applications of AI systems. After his famous loss to IBM's Deep Blue in 1997, Chess Grandmaster Garry Kasparov focused his research on how AI systems can be paired with human decision-makers.[79] Kasparov's research is noteworthy because it acknowledges his personal bias against IBM's Deep Blue and because it explores ways to benefit from machine learning while keeping a human in decision-making processes.[80] Alpha Go, Google Deepmind's AI system that famously beat the world's best Go player in 2015, was a breakthrough that shocked many in the AI research community.[81] When IBM's Watson won the game show Jeopardy in 2011, beating two previous champions, the general population took notice, and many articles about AI

---

[74] Bernard Marr, "What Is the Difference between Artificial Intelligence and Machine Learning?," *Forbes*, December 6, 2016, https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/#4705c422742b.

[75] Marr, "Deep Learning, Machine Learning and AI."

[76] Marr, "Artificial Intelligence and Machine Learning."

[77] Janine Sneed, "AI, Machine Learning and Deep Learning: Is There Really a Difference?," Medium, November 27, 2017, https://medium.com/cognitivebusiness/ai-machine-learning-and-deep-learning-is-there-really-a-difference-5631285052e4.

[78] Sneed.

[79] Kasparov and Greengard, *Deep Thinking*.

[80] Ranger, "Garry Kasparov Is Surprisingly Upbeat."

[81] Jōichi Itō and Jeff Howe, *Whiplash: How to Survive Our Faster Future* (New York: Grand Central Publishing, 2016), loc. 237 of 318, Kindle.

technology were written in a wide range of publications. The majority of these articles lack substance on AI development trajectories and offer little insights for academic research. However, some researchers in examining the achievements of Alpha Go and Watson have determined that significant AI breakthroughs may become more commonplace. Timothy Revell, a science writer for *New Scientist* magazine, notes that an AI system designed by Google's Deepmind passes an aptitude test that suggests AI is becoming more human-like.[82] Christine Horton, a British cybersecurity expert, believes that the hype around AI developments underscores the potential for human augmentation and the ability for society to partner with learning computer systems.[83]

AI systems will be integrated into a wide range of hardware and software systems, and projections on how AI will change our lives are relevant to this thesis given that cybercriminals will likely use these connections against us. Research by Thomas Arnold, Daniel Kasenberg, and Matthias Scheutz is applicable to this thesis; they argue that machine ethics is critical to all AI designs given the likely widespread adoption of AI systems.[84] Peter Asaro, a philosopher of technology at Stanford Law School's Center for Internet and Society, is one of many ethicists concerned that AI systems will be incorporated into weapons systems, dramatically shifting future armed conflicts.[85] Noah Goodall, a Professor at the University of Virginia and a senior transportation researcher for the Virginia Transportation Research Council, has conducted research into ethical decision-making for autonomous vehicles, which he claims have the potential to affect a wide range of autonomous systems. He argues that AI systems in autonomous vehicles will

---

[82] Timothy Revell, "DeepMind AI Is Learning to Understand the 'Thoughts' of Others," *New Scientist*, February 28, 2018, https://www.newscientist.com/article/mg23731673-400-deepmind-ai-is-learning-to-understand-the-thoughts-of-others/.

[83] Christine Horton, "Artificial Intelligence: Separating Hype from Reality," Channel Pro, January 12, 2018, https://www.channelpro.co.uk/advice/10702/artificial-intelligence-separating-hype-from-reality.

[84] Thomas Arnold, Daniel Kasenberg, and Matthias Scheutz, "Value Alignment or Misalignment—What Will Keep Systems Accountable?" (workshop at the 31st AAAI Conference on Artificial Intelligence, San Francisco, CA, 2017), https://aaai.org/ocs/index.php/WS/AAAIW17/paper/view/15216.

[85] Asaro, "On Banning Autonomous Weapon Systems."

have to make life-and-death decisions based on rapidly changing driving situations.[86] As AI systems become more integrated into technologies and equipment used on a daily basis, the implications of aggregating new data sources with machine-learning algorithms will be an issue for continuing research.

D. MALICIOUS USE OF ARTIFICIAL INTELLIGENCE SYSTEMS

Research into the potential malicious uses of AI is a relatively new subset of the AI research community, and multiple universities and institutions are focusing on safety designs for AI. Many researchers and ethicists argue that malicious AI is a potential byproduct of ethical research and that computer scientists should be more aware of the unintended consequences of their research.[87] Machine-learning tools that produce deepfakes—a set of techniques that synthesize new visual products by replacing faces in original files—have garnered broad media attention, and almost weekly, a major news organization publishes a story about the potential dangers of deepfakes.[88] A broad spectrum of scientific fields agrees that AI systems need to be designed with goals and ethics that mirror human values, or "value alignment," to minimize the risks of malicious AI.[89]

One report, in particular, was foundational for this thesis. In February 2018, seven research institutes and 26 researchers published a comprehensive study that examined how malicious AI could be created and how to mitigate the risks associated with it.[90] This report should form the basis of future academic research into malicious AI—the breadth of expertise used in the study ensured that a broad range of factors was considered in the report's analysis. Research by Federico Pistono and Roman Yampolskiy is also valuable because they argue that AI systems may become dangerous at multiple stages of development, and ethical safeguards need to be employed throughout the scientific process

---

[86] Noah J. Goodall, "Machine Ethics and Automated Vehicles," in *Road Vehicle Automation*, ed. Gereon Meyer and S. Beiker (Cham, Switzerland: Springer, 2014), 93–102, https://doi.org/10.1007/978-3-319-05990-7_9.

[87] Pistono and Yampolskiy, "Unethical Research."

[88] Luciano Floridi, "Artificial Intelligence, Deepfakes and a Future of Ectypes," *Philosophy & Technology* 31, no. 3 (September 2018): 317–21, https://doi.org/10.1007/s13347-018-0325-3.

[89] Tegmark, *Life 3.0*, 330.

[90] Brundage et al., *The Malicious Use of Artificial Intelligence*.

of AI design.[91] Yasmin Tadjdeh, a senior editor and researcher at *National Defense* magazine, believes that vulnerabilities exist at multiple phases of AI research, design, and implementation and that organizations need to consider safety as they employ AI in their operations.[92]

Deepfake videos have received extensive media coverage, and most of the related research focuses on the technologies used to create them, methods for detection, privacy concerns, and the implications for public trust in government institutions. Although some deepfakes are humorous, others are terrifying violations of privacy or brand image and have serious emotional impacts for the victims. Figure 2 is an example of a highly sophisticated deepfake video that combined the face of Steve Buscemi with the body of Jennifer Lawrence.

---

[91] Pistono and Yampolskiy, "Unethical Research."

[92] Yasmin Tadjdeh, "AI: A Tool for Good and Bad," *National Defense* 102, no. 774 (May 2018): 10, ProQuest.

Figure 2. Photographs of Jennifer Lawrence and Steve Buscemi (Top) and Deepfake Video Combining Their Images (Bottom)[93]

Although this video was obviously fake and was the product of machine-learning tools, security experts are concerned that these videos will increasingly become more sophisticated and difficult to detect.[94] Some researchers fear that deepfake technology could be used to target government intuitions and diminish public trust. Robert Chesney and Danielle Citron argue that although Deepfake technologies were not used in the Russian hack and release of doctored documents prior to the 2017 presidential election in

[93] Source: Dave Fawbert, "This Deepfake Mashup of Jennifer Lawrence and Steve Buscemi Is Utterly Terrifying," Short List, accessed March 10, 2019, https://www.shortlist.com/tech/deepfake-mashup-jennifer-lawrence-steve-buscemi/379641; and "Deepfake Technology Uses Artificial Intelligence to Superimpose Steve Buscemi onto Jennifer Lawrence in New Video," *Techeblog*, January 31, 2019, https://www.techeblog.com/deepfake-artificial-intelligence-steve-buscemi-jennifer-lawrence/.

[94] Mikael Thalen, "Jennifer Buscemi Is the Deepfake That Should Seriously Frighten You," Daily Dot, January 30, 2019, https://www.dailydot.com/debug/jennifer-buscemi-deepfake/.

France, deepfake videos are the next logical step in Russian efforts to use social media to undermine western democracies and the United States.[95]

There is growing research into methods for detecting deepfakes and for training machine-learning tools to identify false videos. Darius Afchar et al.—computer scientists and machine-learning researchers—have built a video forgery detection network that successfully detects 98 percent of the deepfake videos it processes.[96] David Güera and Edward Delp, researchers at the Video and Image Processing Laboratory at Purdue University, have also developed methods for detecting deepfakes using neural networks to analyze and classify whether a video has been subject to manipulation.[97]

There has been significant news coverage on privacy concerns and the broader implications of deepfakes. Figure 3 is an example of a celebrity whose likeness was used to create a pornographic deepfake video without her consent.[98] Robert Chesney and Danielle Keats are researching the privacy implications of creating fake videos that use a person's image without consent.[99] Their research offers insights into the current legal challenges of preventing the creation of pornographic or personally damaging deepfakes. Chesney and Keats also examine the geopolitical implications of nation-states using deepfake videos as tools to influence public opinion and as a method for psychological operations.[100]

---

[95] Citron and Chesney, "Deepfakes and the New Disinformation War."

[96] Darius Afchar et al., "MesoNet: A Compact Facial Video Forgery Detection Network," Research Gate, September 4, 2018, https://www.researchgate.net/publication/327435226_MesoNet_a_Compact_Facial_Video_Forgery_Detection_Network.

[97] David Güera and Edward J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks" (paper presented at the 15th IEEE International Conference on Advanced Video and Signal Based, Auckland, New Zealand, November 27–30, 2018), https://doi.org/10.1109/AVSS.2018.8639163.

[98] Kelly Earley, "What Is 'Deepfake' Porn and Why Is Scarlett Johansson Speaking Out about It?," Daily Edge, January 2, 2019, http://www.dailyedge.ie/why-scarlett-johansson-is-speaking-out-about-deepfake-porn-4419670-Jan2019/.

[99] Citron and Chesney, "Deepfakes and the New Disinformation War."

[100] Citron and Chesney.

Figure 3. Photograph (Left) and Deepfake Video (Right) of Daisy Ridley[101]

Research by Max Tegmark and the Future of Life Institute advocate for ethics and value orientation to be built into AI systems to help minimize the risks of malicious AI. The Future of Life Institute has hosted three conferences—two in Puerto Rico and one in Monterey, California—that examine, among other topics, methods for ensuring AI research focuses on ethical responsibility and goal orientation. Thomas Arnold, Daniel Kasenberg, and Matthias Scheutz, computer scientists and researchers at Tufts University, have examined methods for building value alignment into machine-learning systems. Miles Brundage, a researcher at Open AI, has published extensively on AI ethics, arguing that designing ethics into computer systems does not always translate into ethical behavior.[102] This line of research is important to this thesis because it highlights the challenges of developing machine-learning tools that avoid being used for malicious purposes.

E. CHAPTER SUMMARY

This chapter highlighted the diverse views that exist among scholars studying AI and its sub-fields as well as the potential impact of emerging AI technology on society in the coming years. In developing the four scenarios in the next chapter and the tactical and strategic responses in the subsequent chapters, this thesis drew on some of the most drastic

[101] Source: Justin Kroll, "Daisy Ridley to Star in Spy Movie 'A Woman of No Importance' for Paramount," *Variety*, January 24, 2017, https://variety.com/2017/film/news/daisy-ridley-a-woman-of-no-importance-paramount-1201968755/; and Megan Farokhmanesh, "Is It Legal To Swap Someone's Face into Porn without Consent?," Verge, January 30, 2018, https://www.theverge.com/2018/1/30/16945494/deepfakes-porn-face-swap-legal.

[102] Brundage, "Limitations and Risks of Machine Ethics."

projections from the scholarly debates discussed in this literature review. TCOs and cybercriminals have demonstrated their ability to adapt to emerging technologies, and illicit online markets will likely be used in future AI-enabled crimes. Views on the future of AI and the technology's impact on society vary greatly, but focusing on the potential dangers of the malicious use of AI seems prudent. Law enforcement agencies and policymakers will need to stay apprised of trends in AI research and the field's development. Finally, the AI research community has begun in recent years to focus on the implications of their research, not to mention the potential harmful adaptations of emerging AI technology. Homeland security officials, across multiple disciplines, should join these discussions to better understand how present-day cybercrime could evolve in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SCENARIOS

> Do you know what is America's greatest export? . . . It is an idea, really. A dream: "Star Trek."
>
> —Singer and Cole,
> *Ghost Fleet: A Novel of the Next World War*[103]

The homeland security enterprise is likely to face a range of complex, criminal threats from AI-enabled cybercrime in the future. This chapter presents four possible future scenarios that forecast what those threats might look like and what challenges law enforcement officials and policymakers could be confronted with. Although these four scenarios are fictitious, they were fabricated from current criminal threats and projections of where AI technology could be within the next several years.

A. SCENARIO 1: AUTONOMOUS WEAPON SYSTEMS

Zhang Wei checked his watch to ensure there was still ample time for all the preparations prior to his flight. This was going to be his largest and most complex score, so he could not afford to make careless mistakes. Zhang Wei had spent nine months preparing the assassination scheme he was minutes from launching, and his journey from promising computer scientist to calculated murderer had occurred without anyone taking notice. Zhang Wei had never been wealthy, but he had been more prosperous than many in his home providence of Guangdong, China. After today, he would be wealthier than any person he had ever known. He was a few hours away from never having to worry about money again.

Zhang Wei checked the access point and refreshed his browser to see the updated prices on the assassination market website. Although this iteration was far more advanced than the first assassination market hosted by Kuabatake Sanjuro on the Dark Net, it

[103] P. W. Singer and August Cole, *Ghost Fleet: A Novel of the Next World War* (Boston: Houghton Mifflin Harcourt, 2015).

followed the same basic principles.[104] The modern version of the assassination market—also hosted on an uncategorized, unlisted, Internet site—could be accessed through a distinct web browser.[105] Users of the site could trust that their identities would be difficult to determine, aided by multi-stage processes and advanced encryption technologies to ensure user anonymity.[106] Zhang Wei even liked that the new site retained the name of its predecessor, ensuring that its legacy was preserved. The current assassination market worked in the same manner as the first site: anyone could nominate a person to be killed with the prediction of the date that the person would die.

Zhang Wei had been watching the market for many months before he had developed his plan. Most of the targets on the site were political figures, politicians, and celebrities. Zhang Wei could not care less about any of them, and he had moved to the United States to study at one of California's most prestigious research universities. He had been certain he would make his fortune in Silicon Valley, but he soon became disillusioned with his life there. The work was hard, the hours were long, and the competition was intense. Zhang Wei had quickly realized that he did not want to follow the pathway of his classmates; he could reach his goals for financial independence by applying his intellect in other ways.

His assassination plan had started nine months ago when he noticed that the Mayor of Los Angeles was on the assassination market. Someone had nominated the mayor to the market following his keynote speech at the Democratic National Convention. Many political pundits considered the mayor a future presidential candidate, and his political views on gun control, immigration rights, and healthcare reform were polarizing public opinion about his potential candidacy. Immediately following the mayor's subsequent interview with one of the Sunday talk shows, during which he had called for the abolishment of the several constitutional amendments, the pledges on the assassination market for his murder started to grow. When the combined value of the mayor's death

---

[104] Bartlett, *The Dark Net*.

[105] Martin, "Lost on the Silk Road."

[106] Martin.

reached Zhang Wei's threshold, he realized he was capable of committing the murder on the prescribed day without anyone knowing he was involved. Zhang Wei did not have anything against the mayor; he generally disliked all politicians regardless of their positions. However, this mayor's political future had ensured that he was a valuable commodity, and Zhang Wei knew he was capable of cashing in.

After confirming the value of the mayor's assassination, he moved onto his weapon system. The real genesis of Zhang Wei's attack planning had not begun on the assassination market; rather, it had been ignited in his computer ethics class. His professor had been lecturing on the updated United Nations ban on autonomous weapons systems, and the class had been reviewing the various arguments for and against the ban. Zhang Wei had always laughed at the first commitments to ban autonomous weapons systems as only countries that lacked the ability to design the systems had signed on.[107] To Zhang Wei, the debate on nations developing autonomous weapons systems seemed meaningless because he knew that he could easily build a weapon system just as deadly as anything that was being debated. He also knew that he did not need Department of Defense funding or research tools—everything he needed could be easily procured. That realization sparked his interest in speeding up his earning potential.

Zhang Wei reviewed the sport aerial drone in his living room, proud of the simple modifications he had made. His drone was popular in the club circles, and many hobbyists valued the model for its prolonged flight capabilities and payload capacity. Other models that were faster, but speed and maneuverability were unnecessary in Zhang Wei's plan. Because this model also possessed a powerful, high-definition camera—the best on the commercial market— even some professional videography companies valued the stock model. The system was perfect for Wei's weaponization plans, affording him the ability to showcase his true masterpiece, his targeting software package.

Zhang Wei had been a gifted computer programmer from a young age, not to mention he was able to purchase software from online illicit markets that would serve his purpose. Facial recognition software was the first easily acquired software package, and

[107] Scharre, *Army of None*.

Zhang Wei modified it to locate targets more quickly within large crowds. Navigation tools that would allow Wei to launch his drown well away from the target location were also easy to procure. The most important software had been designed by Zhang Wei himself; he had been developing deep-learning algorithms that would allow him to track the mayor's travel patterns and frequent movements. When Wei realized the mayor regularly attended professional baseball games, especially on Friday nights, he knew the plan would likely succeed. The mayor's propensity to attend baseball games after a long workweek in an open-air stadium makes a predictable, attractive target for the drone attack.

The last component—the improvised explosive payload—had been the easiest to build but perhaps the most stressful part of the plan. Components were readily available, and Wei learned how to build the device from easily accessible online forums. He elected for simplicity: his drone was outfitted with a small explosive device with metal ball bearings. If he could get his drone within 50 meters of the target, he would likely be successful. The cover of a night baseball game at Dodgers Stadium would allow for the drone to approach the stadium easily, loiter above the stadium lights as it searched for its target, and then drop down quickly to finish its attack programming.

Confident that he had finished all pre-attack preparations, Wei powered down his computer equipment and began to pack. He would fly the next morning from Los Angeles to Thailand and watch the news for the results of his attack. While driving from San Francisco to Los Angeles, Wei deposited his homemade, weaponized drone in a secluded nature reserve, approximately 15 miles east of Chavez Ravine and Dodgers Stadium. At the predetermined hour, the drone would turn itself on and begin its flight toward Dodgers Stadium in search of its target. The drone would hover for approximately 20 minutes searching for the mayor. If the drone located the mayor, it would automatically begin its attack run. If the drone could not find the mayor, it would turn west and fly toward Hawaii until it lost battery power and crashed at sea.

Knowing his attack had a high likelihood of being successful, Wei planned never to return to his apartment or the United States. However, if the attack failed and the drone crashed into the Pacific Ocean, he would return from his vacation and begin working on

his next assassination target. Fortunately, there were plenty of targets available, and Zhang Wei was confident that eventually, his hard work would pay off.

B. SCENARIO 2: DEEPFAKES

Victor reviewed the video again, checking shifts in the light as the faces moved in front of the wide-angle camera. This was a critical aspect of proving the footage was authentic.[108] On a separate screen, Victor checked the audio quality and the tempo of the speakers. His main target had a slower speech pattern than most Americans, so Victor had to account for what would likely be pauses in the dialogue. He stopped the footage and pressed back from his computer screens. The video quality was excellent. You could clearly see his target speaking with two associates in the hotel room. The critical phrases about immigrants were clear and easy to hear. The video would likely shock anyone who saw it. The chief executive officer (CEO) of one of the most popular coffee brands in the world had been caught on camera disparaging immigrants from Latin America and Africa. If the footage were realized on the Internet, it would be devastating in the public arena and have an immediate impact on the CEO's reputation and his company's brand. However, Victor still had to overcome perhaps the hardest challenge of his plan. The footage, although virtually impossible to disapprove, was a fake and a product of advanced computer algorithms and hundreds of hours of videos of the CEO's public-speaking events.[109] Victor was aware that the CEO had been traveling in Europe over the last several weeks, could have been in a hotel room, and could have made the comments to associates. How would the CEO respond to Victor's threat to release the video on a number of decentralized social media platforms?[110]

Victor returned to the Dark Net forums, reading various threads and discussions on new tools. A decade earlier, pioneers in deepfake footage—images or videos that combine

---

[108] Güera and Delp, "Deepfake Video Detection Using Recurrent Neural Networks."

[109] Citron and Chesney, "Deepfakes and the New Disinformation War."

[110] Chris Meserole and Alina Polyakova, "The West Is Ill-Prepared for the Wave of 'Deep Fakes' That Artificial Intelligence Could Unleash," *Order from Chaos* (blog), May 25, 2018, https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash/.

and superimpose different visual and audio files to create new, false videos—attempted to embarrass celebrities by placing their likenesses onto adult film actors.[111] Victor was a big fan of those classic "artists," but he viewed himself as more business savvy. Why go through all the effort of making a high-quality fake video that digital forensics and image analysis could not detect if you were not going to make a profit from your efforts?[112] Today, Victor was using an advancement in video-retargeting technology, which made the creation of his videos quick and cost-effective.[113] But Victor realized he could not focus on his profits yet; he needed to ensure that his fake video would have the required effect. He reread the email he had drafted and double-checked the payment instructions. Victor's criminal scheme was predicated on the belief that the CEO would realize the damage the fake video might cause and would elect to pay Victor to prevent him from releasing the footage. The amount Victor was asking for was a substantial sum of money to be paid via a virtual currency not easily tracked. Victor was betting that the CEO would realize the greater potential risk of the footage being released.

Despite the countless hours spent creating the deepfake video, Victor realized the whole operation would hinge on how the CEO reacted to the demands in the ransom note. Victor's terms were direct—payment within 72 hours of receipt of the email or he would ensure that the footage would go viral. The note also suggested the footage was real so as not to tip the authorities off to its lack of authenticity or the means by which it was created. His scheme was built on the premise that someone could have secretly filmed the CEO making the offensive remarks, and Victor was betting on the premise that society would believe the CEO was capable of saying the things heard in the video.

Victor reviewed the draft email to the CEO's personal email address one last time and then sent the message. Victor powered off the computer equipment, unplugged the multiple routers, and surveyed the apartment. The room was not his, and he doubted that

---

[111] Farokhmanesh, "Is It Legal to Swap Someone's Face?"; and Meserole and Polyakova, "The West Is Ill-Prepared."

[112] Farokhmanesh., "Is It Legal to Swap Someone's Face?"

[113] Rose Eilenberg, "Beyond Deep Fakes: CMU Method Transfers Style from One Video to Another," *University Wire*, September 18, 2018, ProQuest.

he would need to stay with his friend again. As he departed the building and began his walk toward the train station, he looked around his home city of Zagreb, Croatia. He would soon fly to Zurich and then to Southeast Asia. Traveling would give the CEO plenty of time to consider the choice that Victor had given him and Victor time to avoid potential law enforcement complications. If all worked well, in a week, Victor would be a rich man and could start working on his next deepfake extortion scheme.

C. SCENARIO 3: IDENTITY THEFT

Rick awoke later than normal and checked the display on his phone. He would have to leave for the airport soon, but there was still time to validate the work he had performed last night. He was confident it would work, but he was prone to make mistakes when he was tired or rushed. Rick powered on his laptop and reviewed the seven profiles of his latest targets. All of them lived in the United States and had access to information he wanted—information that could be profitable if he but gain access to their accounts and bypass their employers' security protocols. The challenge in Rick's work was crafting the emails he sent his targets, as he would have to persuade them to willingly turn over PII without raising their suspicion. Rick did not have the time to attack the computer networks of the victims' employers. Instead, he wanted to attack the most vulnerable part of the computer networks—the users themselves.[114]

In an earlier era, cybercriminals like Rick called his tactic spear phishing—the collection and use of information specifically relevant to the target to create a customized façade—and victims often fell prey to emails claiming to be a from their respective banks, employers, or other trusted entities.[115] More broadly, Rick's tactics fell into the category of social engineering, and he was excellent at manipulating his victims into revealing confidential and personal information.[116] As a teenager, Rick had idolized notorious cybercriminals and hackers, marveling at their abilities to circumvent security barriers via

---

[114] Jan-Willem Bullee et al., "Spear Phishing in Organisations Explained," *Information and Computer Security* 25, no. 5 (October 3, 2017): 593–613, https://doi.org/10.1108/ICS-03-2017-0009.

[115] Brundage et al., *The Malicious Use of Artificial Intelligence*.

[116] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014).

social-engineering tactics. His hero, Kevin Mitnick, had been one of the most famous hackers in the 1990s and had hacked into phone companies, federal agencies, and numerous private companies.[117] Although Rick's social-engineering techniques were far more sophisticated than anything Mitnick had ever used, they relied on the same principles of behavioral-science research and the belief that people fundamentally want to be liked.[118]

Rick had built on the social-engineering processes and philosophies of the cybercriminals that came before him by leveraging deep-learning algorisms to build complex profiles of his potential victims. Decades earlier, cybercriminals used discarded phone records and bank statements in garbage dumpsters.[119] In today's era of cybercrime, Rick's targeting software could piece together publicly available information, social media activity, and media reporting to help him craft tools to steal the identities of his victims. Additionally, Rick leveraged advanced machine-learning services on Dark Net market places to test and validate code in his tools.[120]

Cybercriminals like Rick could use the identities of their victims for many purposes—mostly financial crimes. Rick's first identity-theft crimes had been simple; he had stolen credit card numbers and posted them on illicit online forums. Those basic crimes had netted Rick a steady illicit income in the hacking world. As Rick matured, he realized there were easier ways to make more money if he were patient and found targets that had access to profitable information.

The alarm clock on Rick's phone buzzed, announcing that he had to hail a cab within 30 minutes if he wanted to arrive at the airport in time for his flight. He slowly and methodically reviewed the seven emails to his potential victims and sent each in turn. Each email was concise, no longer than one paragraph. They were tailored to each victim and contained multiple personal references that were designed to generate a friendly response

---

[117] Mitnick and Simon, *Ghost in the Wires*.

[118] Kevin D. Mitnick, "Are You the Weak Link?," *Harvard Business Review* 81, no. 4 (April 2003): 18–20, EBSCO.

[119] Singer and Friedman, *Cybersecurity and Cyberwar*.

[120] "Cybercriminals Adopting Advances in Artificial Intelligence, Warns Fortinet," Security Asia, November 24, 2017, https://www.networksasia.net/article/cybercriminals-adopting-advances-artificial-intelligence-warns-fortinet.1511493180.

(see Figure 4). All of the emails simply asked for the victim to click on a website or an email hyperlink. The victims would likely never realize that if they accessed the link in Rick's emails, he would gain access to their hard drives.[121] Once he gained access, Rick could launch additional software applications that data-mined for information he could sell on illicit online marketplaces. Protected intellectual property, copyrighted files, proprietary research, and PII would garner high prices depending on the source of information.

```
To: Jane.doe@isp.com
From: Jsmith2025@otherisp.com

Subject: It was great to chat with you last week!!!

Hey Jane! It was so great to meet you last week at the
marketing social at Du Point Circle. I love that spot
and although it is always so crowded, they always have
great specials on their appetizers. I also loved
seeing Mary and it has been ages since she and I been
able to talk. I am not sure if you remember but I
mentioned a new educational opportunity that my agency
is considering offering and I wanted to share it with
you to see what you think. We have to make a decision
soon and I would appreciate your thoughts!

www.womenleadersinmarketing.com

Hope to hear from you soon!
Janet
```

Figure 4. Sample Spear Phishing Email

Rick powered down the laptop, stored his other electronics, and grabbed his coat. His flight to Greece would provide ample time for at least a few of his victims to access the phishing email. After he landed in Athens, he would begin data-mining the information he had gained access to and look for the most profitable information. It would be a slow process and take time to research what he uncovered. However, if he was methodical and diligent, he knew that he would find some valuable nuggets to sell. In the end, a few days

[121] Singer and Friedman, *Cybersecurity and Cyberwar*.

of work and research, mostly performed by deep-learning software, would yield substantial profits and allow Rick to continue his criminal activities.

D. SCENARIO 4: VIRTUAL KIDNAPPING

Carlos awoke to the sounds of the ocean and the warm sea breeze blowing through the wooden shutters of his beachside hotel room. It had been a productive two weeks; the time away in Costa Rica had helped him focus on his part-time profession. Carlos generally enjoyed his day job as a computer programmer in the San Francisco Bay Area, but he had never adjusted to the stress and pressure of the startup industry. Every startup was striving to be the next big technology firm or to develop the latest gadget everyone had to have. Carlos knew there were much easier ways to earn money. He had also come to realize that his part-time job was only partially about the money. He enjoyed the action and the thrill of the heist. As a kid, he had loved the old western movies his grandfather used to watch, especially the train robberies or stagecoach heists. Carlos imagined that the money was merely part of the thrill; the excitement of the robbery must have motivated the bad guys. Carlos fancied himself a modern version of a train robber except, instead of guns or explosives, his weapons were software, his ingenuity, and the stupidity of his victims for posting so much of their personal lives on cyberspace portals.

Although the sun was breaking over the horizon, Carlos had much to accomplish before heading to the airport and flying back to California. He wanted to complete all criminal activity in Central America and dispose of all potential computer forensics that could connect him to his crimes. He reviewed the three targets and was confident that his threats on their lives would be convincing. Carlos had worked diligently to develop deep-learning computer algorithms that were capable of scanning various social media sites for new targets. Carlos took advantage of young college kids, usually women at expensive colleges and universities, with parents who were likely to pay to keep their children safe. He had built his own targeting software that searched through social media posts, pictures, and geolocation tags to build social networks of his potential targets. Building his tool had taken him almost two years, but all of that work was beginning to pay off.

Carlos's deep-learning tool had produced the intended results and could find potential targets based on the information his victims freely posted online. Carlos had gotten the idea for virtual kidnapping after hearing about how one of his cousins in Mexico had been victimized. In his cousin's case, Mexican criminal organizations had physically surveilled the family for months before they sent his aunt and uncle pictures of their son and threatened to kill him if a ransom was not paid. Carlos realized there was no need to surveil anyone; all that he needed was available—if you knew how to compile the information and find the patterns.

His victims fit a specific criterion, and his algorithms found college students who attended one of 23 U.S. universities within 100 miles of the southwest U.S. border. The victims were from wealthy families, had traveled to Mexico in the last nine months, and checked into public locations via social media at least four times per week. The victim's use of social media was critical to building the profiles, and geotags of their locations were vital to anticipating where they would likely be in the future. The ability to build a virtual pattern of life for his victims enabled Carlos to make his threats so convincingly.

Carlos had spent almost as much time drafting the threatening emails as he had building the software to develop his likely targets. Carlos had only a few lines to convey his threats, in a manner that would compel the victims' parents to make immediate payments rather than contact law enforcement authorities. Carlos needed to convey two important points in his ransom letters: the victims' social media activity had made it easy for him to find them, and he was more than capable of doing despicable things to the victims if the ransom was not paid. In addition to building target profiles based on social media activity, Carlos was also able to convince families of how dangerous he could be using social media postings from some of Mexico's most notorious cartel hitmen.[122] Carlos would ensure that the victims' parents would receive some of the latest footage of cartel violence when he sent his ransom notes.

---

[122] Joseph Cox, "Mexico's Drug Cartels Love Social Media," *Vice* (blog), November 4, 2013, https://www.vice.com/en_us/article/znwv8w/mexicos-drug-cartels-are-using-the-internet-to-get-up-to-mischief.

Time was running short, and Carlos double-checked the three victims and the ransom letters for each, which contained the same threat and claimed to be authored by a prominent Mexico-based criminal organization. The letters were concise, contained accurate personal information about the victims, predicted where the victims would be, and threatened to kidnap the victim if a large ransom was not paid within 96 hours of the receipt of the message. All of the victims' parents—the recipients of Carlos's letters—were extremely wealthy and had no notable connections to U.S. law enforcement. Perhaps they would pay the ransom, but it really did not matter. The victims were not in any real danger, and Carlos had no intention or capability of actually harming them. But their parents did not know that.

Carlos was confident in his work and sent the emails to parents of the three victims. After verifying that the messages were sent, he powered off the computer and withdrew the external storage device containing all of the victims' targeting information. All of his software had been developed on his vacation, so there was no evidence of his work at home in California. He put the computer and storage device in a bag and headed down to the beach. He borrowed one of the resort kayaks and took to the surf for his morning paddle, just as he had done every morning of his vacation. After 20 minutes and about 500 yards from the shoreline, he began dropping his computer hardware into the ocean. He had already deleted the data, but the salt water would soon destroy all of the hardware and remove any traces of his activity. As he turned back toward the beach resort, he began thinking about how he would spend the ransom money he was likely to earn. He would wait for months, maybe years, before he would access any of the ransom money, which was to be paid via cryptocurrency. The wait did not matter—Carlos had time and plenty of potential new victims to find.

E. CHAPTER SUMMARY

AI-enabled cybercrime is likely to present new and more complicated challenges for the homeland security enterprise in the coming years. The four scenarios in this chapter projected potential threats on the horizon that require an examination of how law enforcement officials and policymakers will confront cybercrime. The next chapters

explore potential tactical responses to the threats highlighted in the scenarios and analyze how law enforcement officials can prepare for the future malicious use of AI.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TACTICAL AND OPERATIONAL RESPONSE

> When the past is always with you, it may as well be present; and if it is present, it will be future as well.
>
> —William Gibson, *Neuromancer*[123]

Although many of the challenges highlighted in the four scenarios may be on the distant horizon, law enforcement strategies that are used today may be suitable for responding to future AI-enabled cybercrimes. Moreover, law enforcement and intelligence officials must continuingly educate themselves on emerging AI technologies and their potential for malicious use.[124] The law enforcement strategy of intelligence-led policing (ILP)—a decision-making process that uses criminal intelligence analysis to reduce crime and measure the effectiveness of policing strategies—can be applied to efforts to combat AI-enabled cybercrime.[125] Law enforcement officials will ultimately need to identify individuals suspected of committing future cybercrimes, and investigations that successfully lead to prosecutions and convictions will be an important deterrence. Crimes committed using malicious AI will test law enforcement officials in new ways, so enhanced interagency cooperation will be vital to responding to new criminal threats. Finally, the virtual nature of cybercrime challenges physical jurisdictions, so law enforcement officials will need to rely on international partnerships to build effective investigations.[126] This chapter discusses how law enforcement officials can learn about emerging AI technologies and how they can adapt existing law enforcement tactics and strategies to confront future AI-enabled cybercrimes.

---

[123] William Gibson, *Neuromancer* (New York: Penguin Books, 2016).

[124] Thomas J. Holt and Adam M. Bossler, "Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments," *CyberPsychology, Behavior & Social Networking* 15, no. 9 (September 2012): 464–72, https://doi.org/10.1089/cyber.2011.0625.

[125] Jerry H. Ratcliffe, "Intelligence-Led Policing," *Trends & Issues in Crime and Criminal Justice*, no. 248 (April 2003): 1–6, https://aic.gov.au/publications/tandi/tandi248.

[126] Todd G. Shipley and Art Bowker, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace* (Rockland, MA: William Andrew, 2013), 13, ProQuest.

A. EDUCATING LAW ENFORCEMENT ON CYBERCRIME AND EMERGING AI TECHNOLOGIES

The current cybercrime environment already presents complex challenges for public security officials, and these challenges will be further complicated if cybercriminals adapt AI to their operations. Many law enforcement agencies question their roles in investigating cybercrime, and developing the necessary technical expertise can be challenging.[127] In one study, researchers found that many local law enforcement officials lacked not only adequate training to police cybercrime but also a strong interest in developing the expertise required.[128] The same study concluded that the general profile of law enforcement officials who are interested in investigating cybercrime are older, have little to no previous computer training, and believe that cybercrime is an important issue for their departments.[129] Interest in learning about AI technologies and their potential use by cybercriminals will likely be an important factor when law enforcement and intelligence managers determine which personnel to assign to malicious AI-related investigations.

Although training on artificial intelligence technology may be acquired via books, classroom instruction, and other traditional training methods, some technologies may require other non-traditional training methods. In the deepfake scenario, Victor was able to build false videos from tools he likely learned about online and via hobby forums. Today's deepfake videos are often created by amateurs, and making fake videos of celebrities may not violate current laws.[130] Law enforcement officials, assigned to investigate extortion or cyberbullying crimes related to deepfakes, can develop expertise by joining online forums and participating in amateur video creation.

The autonomous weapon system scenario may also be a situation for which law enforcement can prepare via hobby clubs although formal drone pilot training is available

---

[127] Adam M. Bossler and Thomas J. Holt, "Patrol Officers' Perceived Role in Responding to Cybercrime," *Policing* 35, no. 1 (March 2012): 165–81, https://doi.org/10.1108/13639511211215504.

[128] Holt and Bossler, "Predictors of Patrol Officer Interest in Cybercrime."

[129] Holt and Bossler.

[130] Farokhmanesh, "Is It Legal to Swap Someone's Face?"

for a wide variety of legitimate applications.[131] Although the scenario included an AI-enhanced targeting system, law enforcement officials are researching ways to enforce no-fly areas and methods to safely capture drones that present a public safety threat.[132] Law enforcement officials gain expertise easily on drone operations by attending training and staying abreast of changing legal requirements that may be issued by the Federal Aviation Administration.

Law enforcement and intelligence officials may also be able to leverage partnerships with private industry to develop expertise on the technologies being used by cybercriminals. Several successful partnership models currently exist, and law enforcement and the intelligence community could use relationships from Information Sharing and Analysis Centers (ISACs) to maintain awareness of emerging AI technology.[133] According to their National Council, there are 20 sector-specific ISACs, that support the nation's critical infrastructure and provide information and analytic capabilities to both the private sector and government.[134] In particular, the Financial Services ISAC and the Research and Education Networking ISAC have provided actionable information to help mitigate threats to their respective business operations.[135]

B. ADAPTING ILP TO THE MALICIOUS AI THREAT

The concept of ILP was first referenced in the United Kingdom in the early 1990s. The National Criminal Intelligence Service lists four elements of effective intelligence-led

---

[131] Debbie Kelley, "Colorado Springs Middle-Schoolers Learn Drone Technology in New Flight and Space Class," *Colorado Springs Gazette*, October 10, 2018, https://gazette.com/education/colorado-springs-middle-schoolers-learn-drone-technology-in-new-flight/article_66c9e6e4-cbf8-11e8-898c-27c046bb3b4a.html.

[132] "House Passes Critical Countering Drone Legislation in FAA," Official Website of Congressman Michael McCaul (press release, September 26, 2018), https://mccaul.house.gov/media-center/press-releases/house-passes-critical-countering-drone-legislation-in-faa.

[133] Ron Plesco and Phyllis Schneck, "Criminal Public-Private Partnerships: Why Can't We Do That?," *Georgetown Journal of International Affairs* (Fall 2011): 151–54, ProQuest.

[134] "Member ISACs," National Council of ISACs, accessed October 14, 2018, https://www.nationalisacs.org/member-isacs; and "Information Sharing and Analysis Centers (ISACs) and Their Roles in Critical Infrastructure Protection," National Council of ISACs, January 2016, https://docs.wixstatic.com/ugd/416668_2e3fd9c55185490abcf2d7828abfc4ca.pdf.

[135] Plesco and Schneck, "Criminal Public-Private Partnerships."

policing: targeting offenders, managing crime and insecurity in hotspots, investing in series of crimes and attacks that are linked, and applying preventive measures by working with local communities to reduce crime levels.[136] ILP is a collaborative process that begins with gathering a wide range of information and analyzing it for patterns of common activities to better understand the criminal environment.[137] From its inception, ILP has been an evolving concept that offers opportunities for adaptation as the criminal environment changes.[138] A review of how many law enforcement agencies use ILP strategies may offer insights into how these processes can be employed to combat malicious AI in future cybercrimes.

Many law enforcement agencies leverage a form of the CompStat performance management system—short for computer comparison statistics—as part of their ILP strategies.[139] CompStat, first developed by the New York City Police Department in the early 1990s, uses timely intelligence to deploy resources rapidly to high-crime areas to reduce crime.[140] The CompStat process empowers commanders to achieve their crime reduction goals and provides higher-echelon commanders the ability to show accountability for how resources are deployed.[141] CompStat begins with senior leaders establishing performance metrics for reducing crime in their areas of responsibility and investing in computer analytic capabilities that record and analyze crime data from across the respective jurisdiction.[142] Data are collected and analyzed, often on a weekly basis, and then sent to operational-level decision-makers to adjust their enforcement tactics to achieve

---

[136] Ratcliffe, "Intelligence-Led Policing."

[137] Ray Guidett et al., *New Jersey State Police Practical Guide to Intelligence Led Policing* (New York: Manhattan Institute for Policy Research, September 2006), https://www.nj.gov/njsp/divorg/invest/pdf/njsp_ilpguide_010907.pdf.

[138] Jerry Ratcliffe, *Intelligence-Led Policing*, 2nd ed. (New York: Routledge, 2016), 64.

[139] William F. Walsh, "CompStat: An Analysis of an Emerging Police Managerial Paradigm," *Policing: An International Journal* 24, no. 3 (2001): 347–62, https://doi.org/10.1108/13639510110401717.

[140] Police Executive Research Forum, *CompStat: Its Origins, Evolution, and Future in Law Enforcement Agencies* (Washington DC: Bureau of Justice Assistance, 2013), https://www.bja.gov/publications/perf-compstat.pdf.

[141] Jeffrey S. Magers, "CompStat: A New Paradigm for Policing or a Repudiation of Community Policing?," *Journal of Contemporary Criminal Justice* 20, no. 1 (February 2004): 70–79, https://doi.org/10.1177/1043986203262312.

[142] Walsh, "CompStat."

reduction goals for organizational crime.[143] CompStat's reliance on data analysis is an important aspect to consider when evaluating how to apply it to AI-enabled future cybercrimes. If law enforcement agencies that rely on CompStat to drive their ILP strategies are going to confront malicious AI, then capturing data for timely analysis will be an important investigative requirement.

If ILP and the CompStat process begin with establishing organizational goals, then law enforcement officials will need to gather data and intelligence on malicious AI-enabled cybercrime. In scenario three, Rick uses deep-learning AI to develop detailed patterns of life of his potential victims for spear phishing attacks. Although Rick's tools are hypothetical, the process of social engineering has been used by criminals committing identity theft for decades.[144] By examining how law enforcement currently investigates the interrelationship of identity-related crime, Internet crime, and fraud, we can identify the types of data and reporting that are needed for investigating AI-related crime.[145]

---

[143] Walsh.

[144] Mitnick, "Are You the Weak Link?"

[145] Yvonne Jewkes and Majid Yar, eds., *Handbook of Internet Crime* (Cullompton, England: Willan Publishing, 2010), 275.

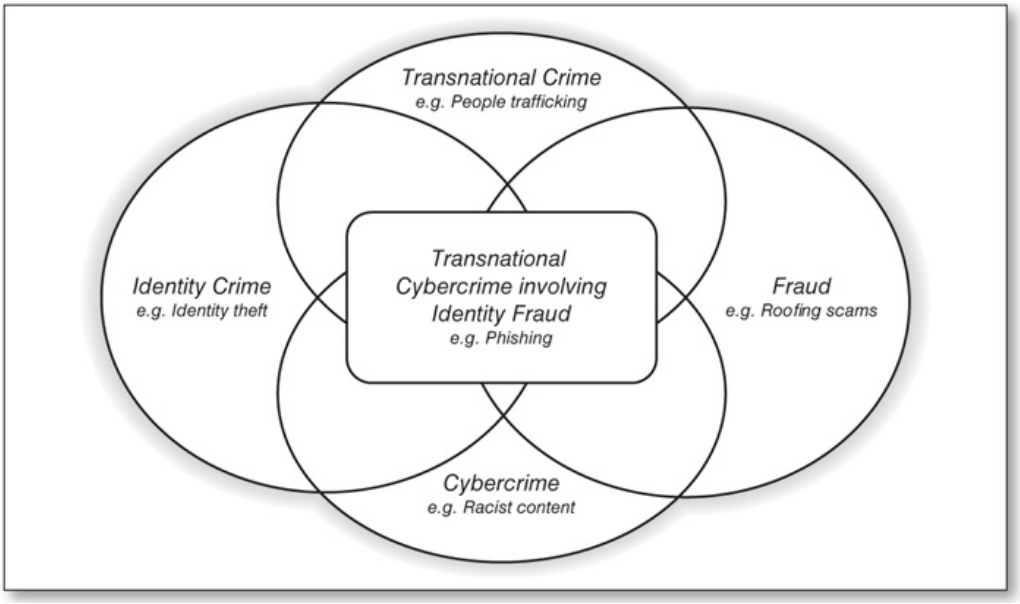

Figure 5. The Interrelationship between Transnational Crime, Identity Crime, Cybercrime, and Fraud[146]

Figure 5 highlights the overlapping nature of these crimes for the purposes of reporting requirements and data needed for a CompStat model. In scenario three, Rick sends spear phishing emails to seven potential victims. Law enforcement officials should examine the digital forensics of any successful or unsuccessful phishing attack to help develop indicators of criminal activity.

In scenarios one and three, the assailants used the Dark Net and online illicit markets to support their illegal activities. Law enforcement and intelligence officials would need effective methods for monitoring activities on these forums to develop a baseline model for measuring change. Unfortunately, the monitoring of online illicit markets—where personal information gathered via phishing attacks is likely sold—is extremely difficult, and online scraping tools used to measure activity have shortcomings.[147] Additionally, when law enforcement has been able to disrupt online illicit markets, as the

[146] Source: K.-K. R. Choo and R. G. Smith, "Criminal Exploitation of Online Systems by Organised Crime Groups, "*Asian Criminology* 3 (2008): 37–59.

[147] Heath-Ferguson, "Offline 'Stranger' and Online Lurker."

FBI did with the Silk Road market in 2013, other markets quickly arise as replacements.[148] If law enforcement investigators are going to effectively police future AI-enabled cybercrime, developing an understanding of illegal activity on the Dark Net will be vital.

Law enforcement agencies are increasingly embracing forms of open-source intelligence (OSINT) as an effective tool for gathering information about online criminal activities.[149] OSINT is generally defined as intelligence collected from sources—such as academic publications, newspapers, social media, and publicly available information—that are open and accessible to the general public.[150] Some law enforcement agencies actively use OSINT in their investigations of violent crimes and are attempting to use social media monitoring as a way to anticipate future crimes.[151] As cybercriminals embrace AI software in their activities, law enforcement officials could explore OSINT capabilities and determine how best to integrate OSINT into their enforcement operations.

C. ENVIRONMENT OF AI-ENABLED CYBERCRIME

Present-day cybercriminals operate on the Dark Net, which is a smaller aspect of the deep web. The deep web contains about 90 to 94 percent of total online content including sites that are not cataloged or indexed.[152] The deep web includes all content that Google and other search engines have not indexed and for which they cannot return search results.[153] The deep web also hosts a wide range of legitimate and private data ranging from

---

[148] Masarah Paquet-Clouston, David Decary-Hetu, and Olivier Bilodeau, "Cybercrime Is Whose Responsibility? A Case Study of an Online Behaviour System in Crime," *Global Crime* 19, no. 1 (2018): 1–21, https://doi.org/10.1080/17440572.2017.1411807.

[149] Edward J. Appel, *Internet Searches for Vetting, Investigations, and Open-Source Intelligence* (Boca Raton, FL: CRC Press, 2011), 11.

[150] Robert Layton and Paul A. Watters, *Automating Open Source Intelligence: Algorithms for OSINT* (Rockland, MA: William Andrew, 2015), ProQuest.

[151] Gabe Rottman, "Open Source Intelligence and Crime Prevention," *Free Future* (blog), December 21, 2012, https://www.aclu.org/blog/national-security/privacy-and-surveillance/open-source-intelligence-and-crime-prevention.

[152] George Hurlburt, "Shining Light on the Dark Web," *Computer* 50, no. 4 (April 2017): 100–105, https://doi.org/10.1109/MC.2017.110.

[153] Digvijaysinh Rathod, "Darknet Forensics," *International Journal of Emerging Trends & Technology in Computer Science* 6, no. 4 (August 2017): 77–79.

corporate intranets to academic journals to social media databases.[154] The Dark Net is a subset of the deep web and has been used for the promotion and distribution of illegal activities.[155]

The deep web and the Dark Net are most often accessed via special search engines that utilize a TOR browser.[156] The TOR browser, designed by the U.S. Naval Research Laboratory, allows for anonymous communications leveraging networks of voluntary nodes that route and encrypt web traffic.[157] TOR conceals communications by selecting random relay nodes to form a complete pathway.[158] This process builds a multi-layered encryption method that makes tracking web traffic extremely difficult.[159] The deep web and Dark Net can also be accessed by lesser-used methods such as I2P and Freenet. I2P was designed as an anonymous peer-to-peer communication pathway that can run a traditional Internet service while Freenet, a predecessor of I2P, uses an unstructured overlay network to protect communications.[160]

Criminals leverage online illicit markets to support a wide range of illegal activities including the smuggling of humans, narcotics, stolen goods, weapons, PII, and intellectual property.[161] The Dark Net of today also offers criminals a wide range of tutorials on how to conduct illicit online activities, and the professional criminal hacking group ShadowCrew offers criminal tutorials on everything from credit card-cloning to the use of cryptography.[162] Future cybercriminals will likely continue to use the Dark Net in their

---

[154] Hurlburt, "Shining Light on the Dark Web."

[155] Zaklina Spalevic and Milos Ilic, "The Use of Dark Web for the Purpose of Illegal Activity Spreading," *Ekonomika* 63, no. 1 (March 2017): 73–82, http://dx.doi.org/10.5937/ekonomika1701073S.

[156] Daniel Sui, James Caverlee, and Dakota Rudesill, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box* (Washington, DC: Wilson Center, October 2015), https://www.wilsoncenter.org/sites/default/files/deep_web_report_october_2015.pdf.

[157] Vincenzo Ciancaglini et al., *Deepweb and Cybercrime: It's Not All about TOR* (Cupertino, CA: Trend Micro, 2013), https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf.

[158] Ciancaglini et al.

[159] Hurlburt, "Shining Light on the Dark Web."

[160] Ciancaglini et al., *Deepweb and Cybercrime*.

[161] Bartlett, *The Dark Net*, loc. 5.

[162] Goodman, *Future Crimes*, loc. 27.

illicit activities, so law enforcement officials will need to identify lead information if they are to investigate AI-enabled cybercrime successfully.

ILP begins with identifying criminal activities, but measuring and analyzing criminal activities via online illicit markets is extremely challenging given the cryptology, privacy measures, and other security protocols being employed on the Dark Net. Online illicit markets use mitigation technologies that make it possible to sell illegal products all over the world and are difficult for law enforcement officials to detect.[163] Markets that specialize in drugs sales on the Dark Net use advanced digital encryption to anonymize the buyers and sellers.[164] Some markets have also decentralized their structure, further complicating law enforcement efforts to investigate and interdict illegal activities.[165] The very nature of the Dark Net, with unknowable realms of password-protected sites, uncategorized websites, and hidden content, provides a space where users can remain hidden.[166] Further complicating investigative efforts, TOR recently added a layer of privacy that makes identifying a website host nearly impossible.[167] If law enforcement officials are to apply their departmental ILP strategies to criminal activities that take place on the Dark Net, they will have to overcome these challenges and identify methods for drawing criminals out of the shadows.

D. IDENTIFYING PERPETRATORS OF AI-ENABLED CYBERCRIME

In 2013, the FBI successfully arrested the owner of one of the most famous online illicit markets on the Dark Net using traditional law enforcement strategies. Beginning in 2011, undercover FBI agents began purchasing illegal goods on the Silk Road, a TOR-based hidden site that allowed users to buy and sell illicit narcotics.[168] The FBI also used

---

[163] D. Decary-Hetu and L. Giommoni, "Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous," *Crime, Law and Social Change* 67, no. 1 (February 2017): 55–75, https://doi.org/10.1007/s10611-016-9644-4.

[164] Martin, "Lost on the Silk Road."

[165] Carlo Morselli and Katia Petit, "Law-Enforcement Disruption of a Drug Importation Network," *Global Crime* 8, no. 2 (May 2007): 109–30, https://doi.org/10.1080/17440570701362208.

[166] Bartlett, *The Dark Net*, loc. 5.

[167] Hurlburt, "Shining Light on the Dark Web."

[168] Bartlett, *The Dark Net*, loc. 136.

undercover agents to pose as assassins and other criminal actors in their investigation into the Silk Road's ringleader, Ross Ulbricht.[169] The investigation was a huge success, resulting in arrests in the United States, the U.K., Sweden, Ireland, Australia, and the Netherlands, and the FBI seized approximately $150 million in bitcoin.[170] The takedown of the Silk Road and Ulbricht also showed that if law enforcement is aware of an online illicit market, it can work with international partners to effectively disrupt and dismantle the criminal enterprise.

Many law enforcement agencies currently confront crime on the Dark Net by adopting practices and techniques of cybercriminals and the hacking community. Some departments have used widely available and published hacking techniques to help penetrate the layers of anonymity provided by the TOR browser.[171] In 2012, the FBI used the Metasploit application to identify the cybercriminals responsible for posting and accessing child pornography on the Dark Net.[172] In 2014, the FBI also participated in an international, multi-agency investigation codenamed Operation Onymous that used hacking tactics and employed malware.[173] Although these tactics have proven successful in identifying cybercriminals on the Dark Net, they do raise ethical and privacy concerns that law enforcement officials will have to consider. Privacy advocates are concerned about potential breaches of First Amendment–protected online speech and how law enforcement monitors the Internet and social media.[174] Law enforcement officials will have to consider the privacy implications of using hacking tools, so operations are conducted within legal frameworks that protect individuals' freedom of speech.

---

[169] Bartlett, loc. 140.

[170] Bartlett.

[171] Andrew Mckinnon, *Hacking: Ultimate Hacking for Beginners, How to Hack* (Scotts Valley, CA: CreateSpace Independent Publishing, 2015), 43.

[172] Metasploit is a penetration-testing platform that allows users to find, test, and validate vulnerabilities. In the cited example, the FBI used this tool to penetrate the Dark Web browser and determine the identities of individuals who had posted child pornography online. Sui, Caverlee, and Rudesill, *The Deep Web and the Darknet*.

[173] Sui, Caverlee, and Rudesill.

[174] Rottman, "Open Source Intelligence and Crime Prevention."

Law enforcement officials have also partnered with private industry to develop tools for conducting forensic research on the Dark Net and for following the transactions of the cryptocurrencies that form the financial backbone of illicit markets. TOR browser activities can be examined in several ways; security researchers can examine registry changes, network forensics, and the memories of seized computer hard drives.[175] Law enforcement can also examine cryptocurrency transactions, and Internet Evidence Finder, for example, has the ability to recover artifacts from Bitcoin transactions.[176] Academia and private research institutions can also assist in identifying cybercrime, and some scholars have advocated for additional research into the recognition of technology-enabled crime.[177] Dark Net scraping tools can also capture user activity although this method of research has proven extremely time-consuming, and cybercriminals have adapted to detection methods.[178] Law enforcement and security officials will need to focus on understanding and mapping the illegal activity that transpires on the Dark Net if they are to develop detection methods for combatting AI-enhanced cybercrime.

E. INTERAGENCY AND INTERNATIONAL PARTNERSHIPS TO INVESTIGATE MALICIOUS AI

The FBI's investigation and subsequent arrest of Ross Ulbricht and closure of the Silk Road demonstrated the criticality of working across multiple jurisdictions and with international partners. In all four of the fictional scenarios, the criminal actors cross real and virtual borders, using international travel as a means for avoiding law enforcement detection. Present-day cybercriminals benefit from difficulties in tracing their online activities and the challenges in prosecuting them when their activities cross international boundaries.[179] If law enforcement officials are to successfully investigate AI-enabled

---

[175] Rathod, "Darknet Forensics."

[176] Rathod.

[177] Thomas J. Holt, "Regulating Cybercrime through Law Enforcement and Industry Mechanisms," *Annals of the American Academy of Political and Social Science* 679, no. 1 (September 2018): 140–57, https://doi.org/10.1177/0002716218783679.

[178] Christin, "Traveling the Silk Road."

[179] Weiping Chang et al., "An International Perspective on Fighting Cybercrime," in *Intelligence and Security Informatics*, ed. Richard Miranda et al. (Berlin: Springer, 2003), 379–84.

cybercrime, they will almost certainly need to partner with domestic agencies as well as international organizations.

At the federal government level, the FBI leads the National Cyber Investigative Joint Task Force (NCIJTF), which brings together more than 20 partner agencies.[180] The task force approach to investigating cybercrime allows federal agencies to leverage their respective authorities to maximize their effectiveness and ensure that criminals face the most severe penalties possible. At the state and local levels, fusion centers are uniquely positioned to support cybercrime investigations by promoting information-sharing, analyzing data, and disseminating conclusions from completed investigations to a wide audience.[181] In 2015, fusion centers in Florida, Louisiana, and Southern California shared information on a sex-trafficking ring that led to the arrest of three individuals.[182] This collaboration shows the need for effective information sharing across law enforcement jurisdictions to investigate cybercrime successfully.

At the international level, the International Crime Police Organization (INTERPOL) and the European Union Agency for Law Enforcement Cooperation (EUROPOL) support investigations that span multiple law enforcement jurisdictions. In its 2018 threat assessment on Internet-organized crime, EUROPOL highlights the importance of collaborating with law enforcement, the private sector, and academia to combat cybercrime.[183] The report also notes that emerging technologies such as artificial intelligence will challenge law enforcement capabilities and that security personnel should focus on understanding how AI will impact future crime. INTERPOL has also developed the Global Complex for Innovation to focus on identification of criminal activities as well

---

[180] "National Cyber Investigative Joint Task Force," Federal Bureau of Investigation, accessed December 3, 2018, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

[181] Department of Justice, "Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers," May 2015, https://it.ojp.gov/GIST/178/Cyber-Integration-for-Fusion-Centers--An-Appendix-to-the-Baseline-Capabilities-for-State-and-Major-Urban-Area-Fusion-Centers.

[182] "2015 Fusion Center Success Stories," Department of Homeland Security, September 4, 2015, https://www.dhs.gov/2015-fusion-center-success-stories.

[183] European Union Agency for Law Enforcement Cooperation, *Internet Organized Crime Threat Assessment 2018* (The Hague: European Cybercrime Centre, 2018), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment.

as support partner agencies with training and in operations.[184] As emerging technology develops, international partnerships will be vital in effectively investigating and determining attribution in AI-enhanced cybercrime.

F. CHAPTER SUMMARY

It is unclear when law enforcement will be confronted with the situations described in the four scenarios, but today's enforcement tactics can be used to investigate future AI-enabled cybercrimes. Public security officials will need to focus on education and awareness of how emerging technologies, such as artificial intelligence, will affect future crime. ILP is a doctrine that enables decision-making, and its application should be continued when combating cybercrime. Law enforcement investigations will also remain a vital tool in confronting cybercriminals, and identifying suspects in obscure regions of the Dark Net will be paramount to dismantling crime syndicates. The homeland security enterprise will need to share information effectively, both domestically and internationally, to investigate cybercrime.

[184] "The INTERPOL Global Complex for Innovation," INTERPOL, accessed December 3, 2018, https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.

THIS PAGE INTENTIONALLY LEFT BLANK

V. STRATEGY AND POLICY CONSIDERATIONS

> Humanity does not ask us to be happy. It merely asks us to be brilliant on its behalf.
>
> —Orson Scott Card, *Enders Game*[185]

Each of the four scenarios presents a multitude of challenges for strategic planners and policymakers as they consider how best to confront the malicious use of AI. In scenario one, Zhang Wei plots an assassination and gathers software tools to help facilitate his attack via the Dark Net. In scenario two, Victor—based in Croatia—uses publicly available video and audio to blackmail a U.S. citizen. In scenario three, Rick leverages AI and deep-learning technologies to build advanced spear phishing attacks based on the social media postings of his potential victims. In scenario four, Carlos also uses AI and deep-learning tools to develop complete patterns of life for his American victims and social media postings to kidnap them virtually. In all scenarios, the assailants are in other countries or, in the case of Zhang Wei, seeking to travel to locations where U.S. authorities will have difficulty tracking them. An examination of these scenarios highlights specific areas that need strategic focus and policy considerations.

The four scenarios highlight possible future threats that policymakers and strategic planners will likely encounter, and it would be prudent to start asking questions today that shape future strategies. Of the potential questions that a policymaker could ask, the following three questions would likely shape any policy or strategy designed to defeat the malicious use of AI by cybercriminals.

[185] Orson Scott Card, *Ender's Game*, rev. mass market ed. (New York: Tor, 1994), 277.

(1) What elements need to exist in a cybercrime strategy?

(2) How can we work with international partners to arrest and prosecute cybercriminals?

(3) How can we work with private industry to understand the implications and potential malicious uses of emerging technologies?

The process of reviewing these initial questions can help determine what elements are needed in any new strategies or what changes need to be made to existing strategic frameworks. Prior to making recommendations for any changes, it is prudent to review existing U.S. cybersecurity strategies and examine where any current caps may lie. Policy makers and strategic planners should also review how foreign partners have confronted the cybercrime threat and which international relationships can benefit U.S. efforts to combat cybercrime. This chapter examines how the United Kingdom, France, and Australia are combatting cybercrime and what lessons learned can be drawn from their experiences.

B. U.S. CYBERSECURITY STRATEGIES

In all four of the scenarios, the criminals leverage cyberspace to research and develop their attack plans. At the national level, the Bush, Obama, and Trump administrations issued cybersecurity strategies that outline frameworks for protecting U.S. national interests in cyberspace. The *National Strategy to Secure Cyberspace*, issued by the Bush Administration in February 2003, outlines five strategic priorities to reduce cyber threats through training, international partnerships, and engagement with the private sector.[186] The *International Strategy for Cyberspace*, issued by the Obama administration in May 2001, outlines guiding principles for the United States and establishes distinct policy priorities for the government.[187] The *National Cyber Strategy of the United States*

[186] George Bush, *The National Strategy to Secure Cyberspace* (Washington, DC: White House, 2003), https://www.hsdl.org/?view&did=1040.

[187] Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, May 2011), https://www.hsdl.org/?abstract&did=5665.

of America, issued in September 2018 by the Trump Administration, emphasizes strengthening U.S. economic and security interests by investing in cyber defense.[188]

The Bush administration's strategy aligns with the national strategy for homeland security, focusing on building a strategic framework for cybersecurity. The strategy extends the *National Plan for Information Systems Protection*, created during the Clinton Administration, and outlines five national priorities for protecting critical infrastructure from cybersecurity risks, reducing national vulnerabilities to cyber-attacks, and minimizing damage and supporting recovery when cyber-attacks occur.[189] While this strategy establishes the framework for the new federal homeland security infrastructure, it fails to mention cybercrime or criminal activities that are supported in cyberspace. Also, the strategy lacks enforcement mechanisms and requires that voluntary compliance actions be taken by private-sector companies.[190]

The Obama administration's cybersecurity strategy builds on the infrastructure established during the Bush administration and emphasizes partnership-building.[191] To achieve its objectives, the strategy outlines seven policy priorities and highlights the importance of international partnerships and cooperation with foreign governments.[192] The Obama administration's strategy, in contrast to the Bush administration's, specifically mentions cybercrime although it only outlines the rules and international laws U.S. law enforcement must observe.[193]

---

[188] Donald Trump, *National Cyber Strategy of the United States of America* (Washington, DC: White House, September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[189] Andrea Peterson and Sean Pool, "Timeline: U.S. Cybersecurity Policy in Context; A Look at President Obama's Latest Executive Order and the Policies That Preceded It," Science Progress, February 13, 2013, https://scienceprogress.org/2013/02/u-s-cybersecurity-policy-in-context/.

[190] Dan Verton, "Bush's Cybersecurity Plan Falls Short, Report Says," *Computerworld* 36, no. 52 (December 23, 2002): 10, ProQuest.

[191] Ted Gotsch, "Epic Gives Administration Good Marks in Cybersecurity, Less So in Civil Liberties," *Cybersecurity Policy Report* (October 25, 2010), ProQuest.

[192] Obama, *International Strategy for Cyberspace*.

[193] Obama.

The Trump administration's strategy is the first presidential strategy to focus on specific elements of cybercrime and, under its first pillar, to define five priority actions for combatting cybercrime and improving incident reporting.[194] The strategy calls for private industry to provide prompt incident reporting and cites areas where new legislation is needed to modernize electronic surveillance and computer crime laws.[195] Similar to the Bush and Obama administrations' strategies, the Trump administration's strategy builds on the work of past administrations and lacks mechanisms for ensuring the goals and priority actions are carried out.[196] Although the strategy was recently released, the fact that it is the first to highlight cybercrime indicates a growing sense among policymakers that cybercrime is a growing national security threat.

C. CYBERSECURITY VERSUS CYBERCRIME

Although the United States has had cybersecurity strategies for decades, No presidential strategy focuses solely on cybercrime, nor does one officially define the concept.[197] Cybercrime, broadly defined as crimes that involve computers and networks, has been a growing category of crime for the past two decades that impacts individuals, corporations, and governments.[198] Emerging technologies and the expanding trend of interconnected wireless devices offer new opportunities for cybercriminals to exploit growing societal reliance on computer and networked systems. Smartphones, networked personal devices, and Internet-connected appliances in our homes offer cybercriminals new pathways to attack our personal information.[199] Devices that leverage machine-learning

---

[194] Trump, *National Cyber Strategy*.

[195] Trump.

[196] Derek Hawkins, "The Cybersecurity 202: Trump Administration Seeks to Project Tougher Stance in Cyberspace with New Strategy," *Washington Post*, September 21, 2018, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/21/the-cybersecurity-202-trump-administration-seeks-to-project-tougher-stance-in-cyberspace-with-new-strategy/5ba3e85d1b326b7c8a8d158a/.

[197] Kristin M. Finklea and Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement* (Washington, DC: Congressional Research Service, July 20, 2012), 16, 18.

[198] Amit Wadhwa and Neerja Arora, "A Review on Cyber Crime: Major Threats and Solutions," *International Journal of Advanced Research in Computer Science* (2017): 6.

[199] Singer and Friedman, *Cybersecurity and Cyberwar*, 254.

technology and artificial intelligence will soon provide cybercriminals access to our personal lives and identities.[200] Governments around the world are struggling to combat the current threats posed by cybercriminals, and significant attention needs focusing in these areas if we hope to effectively combat cybercrime in the future.

It is difficult to measure the magnitude of the threat from cybercrime given the lack of a comprehensive dataset on cybercrime incidents.[201] According to Symantec Corporation, in 2011, cybercrime resulted in total net losses of $388 billion in 24 countries—although it should be noted that Symantec Corporation offers security solutions, its bias may exaggerate the cybercrime threat environment.[202] Cybercrime transcends international boundaries. *Forbes* reports that by 2021, cybercrime is estimated to have a global financial impact in excess of $6 trillion per year.[203] The costs to private businesses vary, and according to a study published in 2017 by the Accenture and Ponemon Institute, the average cost of cybercrime globally has risen to $11.7 million per organization, a 23 percent increase over the previous year.[204] Cybercrime, by some estimates, yields more illicit profits than international drug trafficking, and on average, someone's identity is stolen every three seconds as a result of cybercrime.[205]

A byproduct of research that further complicates an already complicated cybercrime environment is the criminal who potentially creates malevolent AI. Cybercriminals, motivated by profit, may develop proxy AI systems that mask their involvement and avoid risk and responsibility.[206] The malicious use of AI could threaten digital security, and machines could become as proficient at hacking and social engineering

---

[200] Tadjdeh, "A Tool for Good and Bad."

[201] Finklea and Theohary, *Cybercrime*, 17.

[202] "Cybercrime Report 2011," Symantec Corporation, November 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/assets/downloads/en-us/NCR-DataSheet.pdf.

[203] Nick Eubanks, "The True Cost of Cybercrime for Businesses," *Forbes*, July 13, 2017, https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#302a77694947.

[204] Hilary Tuttle, "Cybercrime Costs Businesses $11.7 Million Per Year," *Risk Management* 64, no. 10 (November 2017): 36, ProQuest.

[205] Wadhwa and Arora, "A Review on Cyber Crime."

[206] Pistono and Yampolskiy, "Unethical Research."

as human cybercriminals.[207] The ability to detect cybercriminal attacks from malicious AI is predicated on an examination of these technologies and their application to existing criminal patterns and activities. Criminals have long demonstrated that they are early adopters of new technologies.[208]

Cybercrime is a global challenge, and an examination of how other partner nations are confronting this epidemic may offer opportunities for reframing U.S. strategies, policies, and policing programs. The United Kingdom and France are the fifth and seventh largest economies in the world, respectively, according to the International Monetary Fund, and an analysis of the policies and strategies of these two nations may offer insights that the United States can incorporate into its enforcement practices.[209] Additionally, given the global nature of cybercrime and transnational organized criminal networks, the United States will continue to need partnerships to effectively combat cybercriminal activities.

D. EXAMINING HOW THE UNITED KINGDOM CONFRONTS CYBERCRIME

The United Kingdom combats cybercrime with a unified organizational construction, a single national strategy that governs specific objectives for achieving cybersecurity, and a view toward working with private industry to understand how criminals will leverage emerging technologies. The United Kingdom's streamlined structure provides for a unified command-and-control apparatus that facilitates accountability and measurement of the country's law enforcement activities. The national strategy for cybersecurity also provides a clear understanding of the threats that the United Kingdom (UK) faces from cybercrime as well as outlines specific methods for policing and engaging with private industry. Identifying both a primary federal agency for cybersecurity and a national strategy also provides a single entity through which private industries work with UK security partners, so private industry can easily identify agencies to engage in efforts to protect their information and report incidents of cybercrime.

---

[207] Brundage et al., *The Malicious Use of Artificial Intelligence*.

[208] Goodman, *Future Crimes*.

[209] "Report for Selected Countries and Subjects," International Monetary Fund, April 2018, https://www.imf.org/external/pubs/ft/weo/2018/02/weodata/index.aspx.

In the United Kingdom, serious organized crimes—such as money laundering, human trafficking, child sex exploitation, and cybercrime—fall under the jurisdiction of the National Crime Agency (NCA).[210] The NCA, much like its counterterrorism partner agency, the Counter Terrorism Command, is based in London and is similar to the Federal Bureau of Investigation in the United States. The NCA is the national lead for investigating cybercriminal activities, working closely with the London Metropolitan Police, the agency responsible for cybercrime investigations in the nation's capital.[211] Within the NCA, the National Cyber Crime Unit works closely with Regional Organized Crime Units (ROCUs), the London Metropolitan Police's Cyber Crime Unit, other British government agencies, international law enforcement partners, and private-sector firms.[212] The National Cyber Crime Unit also manages the Action Fraud web portal, which is a single access point for reporting incidents of cybercrime and computer fraud.[213]

The United Kingdom published its updated five-year National Cyber Security Strategy in 2016, and the strategy focuses on the themes of defending, deterring, and developing as methods for confronting cybercrime.[214] The *National Cyber Security Strategy 2016–2021*, written in plain language and without technical jargon, specifically outlines cybercrime methods, security vulnerabilities, and strategies for improving cybersecurity. The strategy also lays out specific methods in the implementation chapter that multiple agencies in the UK government will undertake to achieve the overall strategic goals outlined in the document. Moreover, the strategy lays out expectations for government agencies, private industries, and individual citizens to combat cybercriminals effectively.[215]

---

[210] Nadav Morag, *Comparative Homeland Security: Global Lessons*, 2nd ed. (Hoboken, NJ: John Wiley & Sons, 2018), 192.

[211] Morag, 192.

[212] "National Cyber Crime Unit," National Crime Agency, accessed August 10, 2018, http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

[213] "What Is Action Fraud?," National Fraud and Cyber Crime Reporting Centre, May 22, 2014, https://www.actionfraud.police.uk/what-is-action-fraud.

[214] Her Majesty's Government, *National Cyber Security Strategy 2016–2021* (London: Stationery Office, November 1, 2016).

[215] Her Majesty's Government.

In addition to the United Kingdom's governmental structure and single national strategy, the island nation has invested in developing cybersecurity expertise that generates institutional knowledge for the British government and private industry. The British government has invested in private startup companies as well as the education system to develop cybersecurity expertise.[216] At the national level, the National Cyber Security Centre (NCSC) has private-sector engagement responsibilities to develop the UK's cybersecurity expertise.[217] Created in 2016, the NCSC has consolidated four other UK organizations with cybersecurity expertise into a single organization to better work with government agencies, private industries, and academic institutions.[218]

E. EXAMINING HOW FRANCE CONFRONTS CYBERCRIME

France uses many of the same methods for combatting cybercrime as the United Kingdom does, but France has a national cybersecurity strategy with specific objectives, a national-level agency for monitoring government computer systems, and a national police force with cybercrime investigative responsibilities. France's national cybersecurity strategy bears similarities to the United Kingdom's strategy; however, France emphasizes the importance of leading the European Union's efforts to protect cyberspace proactively.[219] Although France has a single national-level agency for protecting government computer networks and information systems, several other French agencies have cybersecurity authority.[220] Perhaps one of the most important distinctions of French federal cybersecurity efforts is the amount of emphasis placed on education and the development of cybersecurity expertise, not only in France but throughout the European Union. France's cybersecurity strategies, monitoring agencies, and focus on education closely adhere to recommendations outlined in a 2012 report from the European Network

---

[216] Morag, *Comparative Homeland Security*, 340.

[217] "About the NCSC," National Cyber Security Centre, accessed August 18, 2018, https://www.ncsc.gov.uk/information/about-ncsc.

[218] National Cyber Security Centre.

[219] Morag, *Comparative Homeland Security*, 350.

[220] Morag.

and Information Security Agency that calls for EU members to develop comprehensive cybersecurity strategies.[221]

France's *National Digital Security Strategy* was signed in 2015, outlining five strategic objectives: defend French information networks and critical infrastructure, proactively combat cybercrime, institute cybersecurity training throughout all levels of education, create an environment that encourages and supports cybersecurity research and design in France, and be a driving force in the European Union to promote safe and open cyberspace.[222] France's first and second objectives are similar to the United Kingdom's goals under the deter and defend groupings. However, France's strategy calls for cybersecurity education to be a core curriculum from grade-school age into the college years of French students.[223] France also explicitly outlines its role in the European Union and its commitment to lead cybersecurity initiatives for the EU.

France, similar to the United Kingdom, has established a lead federal agency for cybersecurity although other parts of the French state have cybersecurity responsibilities. The *Agence Nationale de la Sécurité des Systèmes d'information* (French Network and Information Security Agency, or ANSSI) is France's national authority for cybersecurity, and the agency is responsible for preventing and responding to cybersecurity incidents.[224] The French Ministry of Defense also has cybersecurity responsibilities, and in 2017, France created a cyber-command structure with responsibilities for integrating digital warfare into military operations.[225] The French Ministry of the Interior houses the nation's investigative capacities, and the Gendarmerie is the lead federal investigative agency for cybercrime.[226]

---

[221] European Network and Information Security Agency, *National Cyber Security Strategies* (Heraklion, Greece: ENISA, May 2012), https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.

[222] Agence Nationale de la Sécurité des Systèmes d'information, *French National Digital Security Strategy* (Paris: ANSSI, October 10, 2015), https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/.

[223] Agence Nationale de la Sécurité des Systèmes d'information.

[224] "Home Page," Agence Nationale de la Sécurité des Systèmes d'information, accessed August 16, 2018, https://www.ssi.gouv.fr.

[225] Agence Nationale de la Sécurité des Systèmes d'information.

[226] Agence Nationale de la Sécurité des Systèmes d'information.

France's cybersecurity structure in some aspects mirrors the U.S. structure for cybersecurity with multiple agencies having responsibilities for different aspects of cybercrime policy and investigations.

One unique aspect of the French approach to combatting cybercrime is the emphasis on cybersecurity education, training, and development. For several years, France reported some of the highest levels of cybercrime in the European Union, which may have shaped the country's focus on education and cyber hygiene techniques. In 2013, the cybersecurity firm Symantec reported that 41 percent of French smartphone users had been victims of cybercrime compared to 29 percent of other European smartphone users.[227] The Symantec study prompted the head of ANSSI to declare that lowering incidents of cybercrime was critical to the nation's survival.[228] France's focus on education is likely an attempt to increase citizen awareness of cyber hygiene practices that can effectively mitigate many vulnerabilities that foster cybercrime.

France's emphasis on education and developing an environment that supports research and design for Internet technology may help prepare the country from new threats. Emerging technologies—such as artificial intelligence and machine learning, the growing trend of networked devices, and the Internet of things—are likely to expand exploitable pathways for cybercriminals. The ability to detect cybersecurity attacks from malicious AI is predicated on the examination of these technologies and their application to existing criminal patterns and activities. Criminals have long demonstrated that they are early adopters of new technologies.[229] France's emphasis on education and partnerships with institutions that are developing new technologies will likely give the nation and the European Union the opportunity to confront new criminal challenges as they develop.

---

[227] "France Has Most Cybercrime Victims in Europe," RFI, October 3, 2013, http://en.rfi.fr/economy/20131003-france-has-highest-cybercrime-rate-europe.

[228] RFI.

[229] Goodman, *Future Crimes*.

F. WHAT CAN THE UNITED STATES LEARN FROM THE UK AND FRANCE?

A review of how the United Kingdom and France are confronting cybercrime offers multiple best practices for the United States to consider incorporating into its own strategies and cybersecurity initiatives. Unlike the United Kingdom and France, the United States lacks a national cybercrime strategy, although multiple cabinet-level agencies have established strategies. Also, in contrast to the UK and France and likely due to a lack of strategy or doctrine, the United States does not have defined goals or objectives regarding how to confront cybercrime. The United States has numerous agencies at the federal, state, and local levels that are focused on preventing or responding to cybercrime. However, there is not a unity of command or hierarchy for the various agencies to work together to confront complex cybersecurity threats. Finally, the United States has many initiatives to engage with the private industry and academic institutions to learn about threats from emerging technologies. Nevertheless, the United States lacks formal doctrine and unifying guidance to ensure that government entities are working closely with technology experts to understand threats from emerging technologies.

G. AUSTRALIA: A POSSIBLE MODEL FOR TRACKING CYBERCRIME

Australia, like many prosperous countries, has to confront the challenge of cybercrime and develop effective methods for targeting cybercriminals. In 2013, Australia published its first *National Plan to Combat Cybercrime*, and on May 19, 2017, the Australian Department of Home Affairs agreed to develop a new national plan to tackle increasing risks of cybercrime to Australian businesses and citizens.[230] In an effort to understand and track cybercrime in Australia, the government developed the Australian Cybercrime Online Reporting Network (ACORN), so the public can securely report

[230] "Cybercrime," Australian Department of Home Affairs, accessed July 29, 2018, https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security.

instances of cybercrime.[231] ACORN is a key initiative under the new *National Plan to Combat Cybercrime*.[232]

ACORN is part of a national policing initiative, and multiple Australian agencies participated in its design and implementation. All Australian law enforcement agencies participate in ACORN as well as the attorney general's departments; the Australian Communications and Media Authority, Australia's equivalent of the Consumer Protection Agency; and the Office of Children's eSafety Commissioner.[233] ACORN captures a wide variety of cybercrimes ranging from attacks on computer systems to cyber-bullying to identity theft to online child pornography.[234] The use of a common reporting platform that captures a wide range of cybercrime enables law enforcement, public safety officials, and policymakers to develop a comprehensive understanding of crime patterns.

Australia's approach to combatting cybercrime offers several good practices that could be adopted in the United States. Although Australia is roughly the same size as the continental United States, its population is significantly smaller with 89 percent of its 23 million inhabitants residing in urban areas.[235] Australia's smaller urban population can be educated on the government's public safety strategies via marketing campaigns. Advertisements, commercials, and media reporting help provide awareness about the ways Australia is confronting cybercrime. General awareness of government strategies and enforcement programs also allows for citizens and Australia's legislative branches to seek accountability from federal programs.

ACORN is one good practice from Australia that the United States could consider using as a method for tracking and reporting cybercrime. Currently, in the United States, multiple federal agencies have cybercrime responsibilities, and virtually every state has its

---

[231] "About the ACORN," Australian Government, accessed July 29, 2018, https://www.acorn.gov.au/about-acorn.

[232] Australian Government.

[233] Australian Department of Home Affairs, "Cybercrime"; and Australian Government, "About the ACORN."

[234] "Learn about Cybercrime," Australian Government, accessed July 29, 2018, https://www.acorn.gov.au/learn-about-cybercrime.

[235] Morag, *Comparative Homeland Security*, 41.

own cybercrime program. A quick review of the Department of Justice's website shows that depending on the cybercrime, an American citizen would have to contact multiple federal investigative law enforcement agencies.[236] In contrast, Australia has one online platform that all relevant agencies leverage for crime reporting and trend analysis. Australian law enforcement agencies likely have a better understanding of cybercrime in their country compared to U.S. agencies.

Australia's unified national strategy for combatting cybercrime is another good practice that could be adopted in the United States. Under Australia's *National Plan to Combat Cybercrime*, all relevant federal agencies have responsibilities.[237] A single national strategy ensures that all agencies follow the same plan and are responsible for achieving the stated objectives. In contrast, the United States does not have a national strategy for combatting cybercrime, at least to the extent that every federal agency is held accountable in the same fashion, as in the Australian system.[238] In the United States, federal law enforcement agencies have separate and often agency-specific strategies. As a result, it seems more difficult in the United States to measure the performance of individual agencies and their strategies to reduce cybercrime. In Australia, a common strategic focus and ACORN provide a mechanism for evaluating how effective the Australian partner agencies are at reducing cybercrime.

Australia has developed a unified approach at combatting cybercrime and an efficient method for reporting and tracking cybercriminal activity. Australia's *National Plan to Combat Cybercrime* appears to be an effective mechanism for bringing all of Australia's relevant agencies into the same strategic focus. ACORN provides Australian citizens with a straightforward method for reporting a wide range of cybercrimes, and it enables law enforcement to approach cybercrime holistically. Although it would likely be difficult to connect the numerous U.S. law enforcement agencies that have cybercrime

---

[236] "Reporting Computer, Internet-Related, or Intellectual Property Crime," Department of Justice, accessed July 29, 2018, https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime.

[237] Australian Government, "About the ACORN."

[238] Chang et al., "An International Perspective on Fighting Cybercrime."

investigative authorities with a common strategy, the United States should further examine how Australia combats cybercrime and how America can benefit from its strategic approaches.

H. CHAPTER SUMMARY

Policy makers and strategic planners should consider cybercrime as an independent category of criminal activity under the broader issue of cybersecurity. A new strategy for combatting cybercrime should emphasize methods for reporting cybercrime and establishing a baseline reporting system. The United States should examine international law enforcement partnerships and seek opportunities to collaborate on fighting cybercrime. Finally, any new strategic initiatives should emphasize partnering with private industry and academia to ensure that policies stay abreast of current trends and emerging technological developments.

VI. FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

> It occurs to me that our survival may depend upon our talking to one another.
>
> —Dan Simmons from *Hyperion*[239]

A. INTRODUCTION

This thesis asked the questions of how TCOs and cybercriminals might leverage developing AI technology to conduct more sophisticated criminal activities and what steps the homeland security enterprise should take today to prepare. The future of AI-enabled cybercrime was envisioned through the examination of four possible scenarios that leveraged existing criminal patterns to show how criminal activities may evolve. Because cybercrime will become more complicated when criminals incorporate AI into their schemes, homeland security officials, policymakers, private-sector leaders, and academic institutions will need to work together to confront malicious AI. This chapter presents findings from the four future scenarios, conclusions from the tactical and strategic responses to AI in cybercrime, and recommendations for the homeland security enterprise to defeat the threat of future, malicious AI-enabled cybercrime. The end of this chapter suggests areas of future study that were outside the scope of this thesis but deserve additional research and examination.

B. FINDINGS

This thesis finds that the threat posed by malicious AI is most likely to augment existing homeland security and cybercrime threats as opposed to radically change the cybercrime landscape. TCOs and cybercriminals have repeatedly demonstrated the propensity to adopt emerging technologies and, therefore, are likely to incorporate AI software into their criminal operations.[240] Cybercrimes—such as spear phishing, identity

---

[239] Dan Simmons, *Hyperion* (London: Gollancz, 2011).

[240] Goodman, *Future Crimes*, loc. 2.

theft, and social engineering—will continue to challenge the homeland security enterprise and society. Emerging AI technologies will likely offer new access points to target potential victims and will add a new level of sophistication to cybercrime.

C. CONCLUSIONS

Although it is unclear when AI technology will develop to the point that cybercriminals can incorporate new technological tools into their operations, this thesis concludes that the homeland security enterprise needs to immediately start confronting the potential threats posed by malicious AI. Previous research into chess-playing software has demonstrated that advances in cognitive computing can happen rapidly and catch industry experts by surprise.[241] AI systems, which can process and analyze large amounts of medical test results and associated data, are being incorporated into systems that integrate copious amounts of PII via the migration to electronic health records.[242] According to a report published by Allied Market Research in February 2019, global investments in AI research in the medical industry are expected to grow at a combined annual rate of nearly 50 percent from 2018 to 2025, signifying the future integration of AI software systems into one of the largest industries in the United States.[243] Many industries are examining how ML software algorithms can help solve big-data challenges, and AI technology will increasingly be integrated into expanding aspects of modern digital life.[244] Malicious AI may be years or even decades away from being used in cybercrime, but it is prudent for the homeland security enterprise to begin developing strategies today to manage the potential threat, given that AI systems are likely to become a major aspect of our society.

---

[241] Kasparov and Greengard, *Deep Thinking*.

[242] Tim Morris, "Making Sense of Healthcare Data with AI to Improve Patient Care Outcomes," *Digital Health Age* (blog), February 19, 2019, http://digitalhealthage.com/making-sense-of-healthcare-data-with-ai-to-improve-patient-care-outcomes/.

[243] Allied Market Research, "Artificial Intelligence in Medicine Market to Reach $18.12 Billion by 2025 at 49.6% CAGR, Says AMR," Globe Newswire, February 20, 2019, http://globenewswire.com/news-release/2019/02/20/1738362/0/en/Artificial-Intelligence-in-Medicine-Market-to-Reach-18-12-Billion-by-2025-at-49-6-CAGR-Says-AMR.html.

[244] Demirkan, Earley, and Harmon, "Cognitive Computing," 16–20.

TCOs and cybercriminals have demonstrated that they will use technology in new and innovative ways, and AI software will likely be integrated into a wide range of cybercriminal activities.[245] ML systems could be used to analyze large amounts of social media postings and assist cybercriminals in social-engineering efforts. Erynn Tomlinson, a former cryptocurrency executive, had approximately $30,000 stolen from her bank account after hackers used social-engineering methods to gain access.[246] In this instance, hackers reportedly gained access to Tomlinson's PII using methods similar to those of Kevin Mitnick in the 1980s: the hackers repeatedly exchanged text messages with customer service representatives to gain enough PII to access Tomlinson's account.[247] As AI systems develop, cybercriminals will almost certainly incorporate new technology into their criminal activities and use new software tools in long-established criminal tactics.

Law enforcement strategies, such as ILP and CompStat, can form the basis of policing future AI-enabled cybercrime; however, these methods need to be adapted to include indicators of malicious AI use. Education on emerging AI technologies should inform law enforcement's approach to cybercrime. Investigative agencies will need to identify indicators and patterns of AI use among cybercriminals to incorporate useful data into policing models. ILP develops information and data analysis into crime intelligence processes, and law enforcement will need to seek methods for incorporating indicators of malicious AI into ILP processes.[248] Although emerging technologies will challenge law enforcement in new ways, existing enforcement strategies are appropriate tools for confronting these challenges.

---

[245] Ryan D. Jerde, "Follow the Silk Road: How Internet Affordances Influence and Transform Crime and Law Enforcement" (master's thesis, Naval Postgraduate School, 2017), 24.

[246] Charlsie Agro, Tyana Grundig, and Nelisha Vellani, "Social Engineering Is the New Method of Choice for Hackers. Here's How It Works," CBC News, February 8, 2019, https://www.cbc.ca/news/technology/marketplace-social-engineering-sim-swap-hack-1.5009279.

[247] Mitnick and Simon, *Ghost in the Wires*, 53.

[248] Jerry H. Ratcliffe, *Intelligence-Led Policing*.

D. RECOMMENDATIONS

This thesis offers three recommendations for the homeland security enterprise to combat the threat of future AI-enabled crime today. These recommendations form a broad policy and strategic framework for federal, state, and local law enforcement agencies to align their activities. Policy makers and legislators, across all levels of government, can also follow these recommendations to synchronize efforts to combat future cybercrime.

1. Develop Strategies to Combat Malicious AI that Align with the New National Strategy for AI and the National Cybercrime Strategy

On February 11, 2019, the White House issued an executive order that outlined broad, strategic objectives for the United States on the development of artificial intelligence.[249] The executive order calls for an American AI initiative, governed by five principles, to ensure that the United States leads AI innovation, develops a workforce that applies AI technologies in future jobs, and creates an environment of public trust in AI technologies.[250] The American AI initiative instructs federal agencies to dedicate resources to high-priority items that could benefit from future AI technologies.[251] The recently released executive order is a useful framework for executive agencies; however, it lacks recommendations regarding the potential threat posed by the malicious use of AI systems. This thesis recommends that executive branch agencies with cybersecurity authority develop implementation plans to address potential risks from AI-enabled cybercrime.

As discussed in Chapter V, the *National Cyber Strategy for the United States*, issued in September 2018, was the first national strategy in the United States to specifically mention threats posed by cybercriminals.[252] Although cybercrime is addressed, this strategy offers minimal guidance for federal agencies with cybercrime enforcement

---

[249] Donald Trump, "Executive Order on Maintaining American Leadership in Artificial Intelligence," February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

[250] Trump.

[251] Michael Kratsios, "Why the US Needs a Strategy for AI," *Wired*, February 11, 2019, https://www.wired.com/story/a-national-strategy-for-ai/.

[252] Trump, *National Cyber Strategy*.

responsibilities. This thesis recommends that federal agencies develop implementation plans that lay out specific goals and actions to combat cybercrime. Federal agencies should examine how Australia tracks cybercrime, developing methodologies for measuring cybercrime to analyze changes in crime trends and the effectiveness of anti-crime operations. These implementation plans should also factor in emerging technologies, such as AI, and outline how agencies will track changes in cybercrime threats with the development of new technologies.

2. Expand Engagements with Private Industry and Academic Institutions

Many federal law enforcement agencies and intelligence community members have robust initiatives to collaborate with private-sector partners on a wide range of threats to national security. Some programs, such as the Domestic Security Alliance Council, co-chaired by the Department of Homeland Security (DHS) and the FBI, offer forums for exchanging information and sharing expertise.[253] Other programs, such as the DHS Analytic Exchange Program (AEP), fund unclassified, collaborative research by private-sector and government-security experts on emerging threat topics.[254] The Department of Defense in the 2015 *Cybersecurity Strategy* outlines the importance of continuing collaboration with private industries and calls for robust dialogue with non-governmental partners on cyber defense issues.[255]

In 2018, one of the research topics for the DHS Analytic Exchange Program focused on developing standards for AI to help mitigate potential risks posed by dual-use AI technologies.[256] The group—composed of government security experts from the

---

[253] "Front Page," Domestic Security Alliance Council, accessed February 21, 2019, https://www.dsac.gov/front-page.

[254] "Intelligence and Analysis/Private Sector Engagement," Department of Homeland Security, July 30, 2018, https://www.dhs.gov/intelligence-and-analysis-private-sector-engagement.

[255] Department of Defense, *DOD Cybersecurity Strategy 2015* (Washington, DC: Department of Defense, April 17, 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[256] Public-Private Analytic Exchange Program, *AI: Using Standards to Mitigate Risk* (Washington, DC: Department of Homeland Security, 2018), https://www.dhs.gov/sites/default/files/publications/2018_AEP_Artificial_Intelligence.pdf.

intelligence and law enforcement communities as well as private industry and the RAND Corporation—produced an unclassified white paper on its research and presented its findings to senior leaders at the Office of the Director of National Intelligence.[257] AEP research topics are selected annually, and the group is funded only to conduct collaborative research for approximately six months. This thesis recommends that programs, such as the DHS Analytic Exchange Program, be reviewed by senior leaders at federal agencies and more funding and time be dedicated to collaborate on emerging threat issues. Research on AI technology should be a prime topic for additional collaboration, and federal agencies should use the AEP as a potential model for private-sector engagement.

Because the development of AI safety tools will continue to be an important topic in coming years, the homeland security enterprise should engage with private industry and academic centers to participate in dialogues about the creation of these tools. Forums hosted by organizations such as the Future of Life Institute offer opportunities for public security officials to understand how AI technologies are developing and to be a part of the development of new AI safety initiatives. Although the Future of Life Institute's 2018 conference in Puerto Rico on beneficial artificial general intelligence hosted participants from the Office of the Director of National Intelligence, no law enforcement agency participated.[258] This thesis recommends that homeland security officials seek out organizations such as the Future of Life Institute and engage in their collaborative seminars to ensure that homeland security perspectives are included in discussions on the implication of emerging AI developments.

3. Expand Partnerships with International Law Enforcement Organizations to Combat AI-Enabled Cybercrime

In all four of the future scenarios, the criminals leverage international travel as a means to avoid detection from U.S. law enforcement officials and to potentially complicate

[257] Public-Private Analytic Exchange Program, 20.

[258] A review of the conference agenda and the participation list shows that representatives from the Intelligence Advanced Research Projects Activity (IARPA) attended the conference and led discussions on several panels on the first day. IARPA is an organization within the Office of the Director of National Intelligence and it facilitates the transition of research results to IC customers for operational application.

investigations into their criminal activities. Future cybercrimes will become borderless, so law enforcement agencies must adopt an appropriate international response.[259] Partnerships with international law enforcement organizations like INTERPOL and EUROPOL will continue to provide value to U.S.-based cybercrime investigations, and the homeland security enterprise should examine ways to collaborate with international law enforcement partners on the threat of future AI-enabled cybercrime.

A robust network of law enforcement associations that support cybercrime investigations exists in the United States, and many of these groups have connections with foreign law enforcement agencies. The High Technology Crime Investigation Association, the International Association of Computer Investigative Specialists, and many fusion centers within the National Network of Fusion Centers, to name a few, collaborate with foreign law enforcement agencies and associations to combat emerging cybercrime threats. Homeland security officials should leverage these partnerships to expand their focus to the potential of emerging malicious AI and begin discussions into policing strategies and tactics that confront borderless crime in the future.

E. NEXT STEPS FOR FUTURE RESEARCH

This thesis was scoped to examine how TCOs and cybercriminals—motivated by profit—could potentially leverage emerging AI technologies in their operations. As a result, this thesis did not examine how nation-states or non-state organizations could use AI against U.S. interests, nor did it explore the ethical considerations of developing or using AI. The threat of malicious AI use will likely transcend threat actor categories—the United States might see foreign terrorist organizations adopt emerging technologies in their operations. While this thesis has focused on profit motivation as the primary driver for the malicious use of AI, the homeland security enterprise could be confronted by non–criminal focused AI threats.

The framework and methodology of this thesis could be adapted to examine how hostile nation-states or non-state organizations could use emerging AI technologies against

[259] Goodman, *Future Crimes*, loc. 366.

the United States. There has been a recent uptick in media coverage of Chinese investments in AI technologies, and security experts have begun to publicly question how China's focus on developing AI will affect U.S. national and economic security interests.[260] On January 22, 2019, Director of National Intelligence Dan Coats published a four-year strategic plan for the intelligence community that specifically highlights future threats from China's AI development.[261] U.S. counterintelligence officials have also expressed concerns about Chinese students using student visa programs to study in U.S. universities, steal intellectual property, and recruit spies.[262] Issues related to nation states' and non-state groups' use of emerging AI technologies to threaten U.S. interests are worthy of additional study and have direct links to homeland security research.

Other potential avenues for future AI research include the ethical implications of AI development as well as appropriate methods for law enforcement and intelligence officials to monitor and review AI software systems. A growing body of research by computer scientists, ethicists, and privacy advocates examines the ethical implications of AI. Homeland security officials should participate in these debates and add their perspectives from across the diverse range of expertise. Paramount to examining the ethics of AI development is a thorough and thoughtful review of the privacy implications of homeland security officials monitoring online AI systems. PII and other personal information are likely to be integrated into future AI-enabled technologies and hardware. Now is the time to review the implications and legality of how law enforcement officials will examine personal information that underlies AI software.

---

[260] David Ingram, "Trump's Artificial Intelligence Order Lacks Funding but Not a Target—China," NBC News, February 11, 2019, https://www.nbcnews.com/tech/tech-news/trump-s-artificial-intelligence-order-lacks-funding-not-target-china-n970406.

[261] Daniel Holl, "New US Intelligence Strategy Focuses on Cyber Threats and Artificial Intelligence," *Epoch Times*, January 24, 2019, https://www.theepochtimes.com/new-us-intelligence-strategy-focuses-on-cyber-threats-and-artificial-intelligence_2778123.html.

[262] Tal Axelrod, "US Intelligence Accuses China of Using Student Spies to Steal Secrets," *The Hill*, February 2, 2019, https://thehill.com/policy/international/china/428181-us-intelligence-accuses-china-of-using-student-spies-to-steal.

F. CHAPTER SUMMARY

Future AI systems will dramatically change society and become integrated into major facets of our day-to-day lives. This thesis began the examination of how emerging AI technologies could be used for malicious purposes by TCOs and cybercriminals to threaten society in new ways. The threat of criminal actors creating malevolent AI introduces new challenges to present-day cybercrimes; homeland security officials, policymakers, private-sector leaders, and academic institutions will need to collaborate in confronting these threats. Ultimately, the threat to the United States posed by potential AI-enabled cybercrime can be mitigated by understanding how AI systems function and are being developed and by ensuring that the homeland security enterprise becomes an active participant in public policy forums on the future of AI technology.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Afchar, Darius, Vincent Nozick, Junichi Yamagishi, and Isao Echizen. "MesoNet: A Compact Facial Video Forgery Detection Network." Research Gate. September 4, 2018. https://www.researchgate.net/publication/327435226_MesoNet_a_Compact_Facial_Video_Forgery_Detection_Network.

Agence Nationale de la Sécurité des Systèmes d'information. *French National Digital Security Strategy*. Paris: ANSSI, October 10, 2015. https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/.

———. "Home Page." Accessed August 16, 2018. https://www.ssi.gouv.fr.

Agro, Charlsie, Tyana Grundig, Nelisha Vellani. "Social Engineering Is the New Method of Choice for Hackers. Here's How It Works." CBC News. February 8, 2019. https://www.cbc.ca/news/technology/marketplace-social-engineering-sim-swap-hack-1.5009279.

Aguilar, Wendy, Guillermo Santamaría-Bonfil, Tom Froese, and Carlos Gershenson. "The Past, Present, and Future of Artificial Life." *Frontiers in Robotics and AI* 1 (2014). https://doi.org/10.3389/frobt.2014.00008.

Allied Market Research. "Artificial Intelligence in Medicine Market to Reach $18.12 Billion by 2025 at 49.6% CAGR, Says AMR." Globe Newswire. February 20, 2019, http://globenewswire.com/news-release/2019/02/20/1738362/0/en/Artificial-Intelligence-in-Medicine-Market-to-Reach-18-12-Billion-by-2025-at-49-6-CAGR-Says-AMR.html.

Anthony, Andrew. "Max Tegmark: 'Machines Taking Control Doesn't Have to Be a Bad Thing.'" *Observer*, September 16, 2017. https://www.theguardian.com/technology/2017/sep/16/ai-will-superintelligent-computers-replace-us-robots-max-tegmark-life-3-0.

Appel, Edward J. *Internet Searches for Vetting, Investigations, and Open-Source Intelligence*. Boca Raton, FL: CRC Press, 2011.

Arnold, Thomas, Daniel Kasenberg, and Matthias Scheutz. "Value Alignment or Misalignment—What Will Keep Systems Accountable?" Workshop at the 31st AAAI Conference on Artificial Intelligence, San Francisco, CA, 2017. https://aaai.org/ocs/index.php/WS/AAAIW17/paper/view/15216.

Asaro, Peter. "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making." *International Review of the Red Cross* 94, no. 886 (June 2012): 687–709. https://doi.org/10.1017/S1816383112000768.

Asimov, Isaac. *Foundation; Foundation and Empire; Second Foundation; The Stars, Like Dust; The Naked Sun; I, Robot*. Minneapolis: Amaranth Press, 1986.

Australian Department of Home Affairs. "Cybercrime." Accessed July 29, 2018. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security.

Australian Government. "About the ACORN." Accessed July 29, 2018. https://www.acorn.gov.au/about-acorn.

———. "Learn about Cybercrime." Accessed July 29, 2018. https://www.acorn.gov.au/learn-about-cybercrime.

Axelrod, Tal. "US Intelligence Accuses China of Using Student Spies to Steal Secrets." *The Hill*, February 2, 2019. https://thehill.com/policy/international/china/428181-us-intelligence-accuses-china-of-using-student-spies-to-steal.

Barrat, James. *Our Final Invention: Artificial Intelligence and the End of the Human Era*. New York: Thomas Dunne Books, 2013.

Barratt, Monica J., and Alexia Maddox. "Active Engagement with Stigmatised Communities through Digital Ethnography." *Qualitative Research* 16, no. 6 (December 1, 2016): 701–19. https://doi.org/10.1177/1468794116648766.

Bartlett, Jamie. *The Dark Net: Inside the Digital Underworld*. Brooklyn: Melville House, 2015. Kindle.

Bernard Marr. "The Key Definitions of Artificial Intelligence (AI) That Explain Its Importance." *Forbes*, February 14, 2018. https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#6b85868e4f5d.

———. "What Is the Difference between Artificial Intelligence and Machine Learning?" *Forbes*, December 6, 2016. https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/#4705c422742b.

———. "What Is the Difference between Deep Learning, Machine Learning and AI?" *Forbes*, December 8, 2016. https://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference-between-deep-learning-machine-learning-and-ai/#181f5b7426cf.

Bernstein, Amy, and Anand Raman. "The Great Decoupling: An Interview with Erik Brynjolfsson and Andrew McAfee." *Harvard Business Review*, June 1, 2015. https://hbr.org/2015/06/the-great-decoupling.

Bilton, Nick. *American Kingpin: The Epic Hunt for the Criminal Mastermind behind the Silk Road*. New York: Portfolio/Penguin, 2017.

Booch, G. "I, for One, Welcome Our New Computer Overlords." *IEEE Software* 32, no. 6 (November 2015): 8–10. https://doi.org/10.1109/MS.2015.134.

Bossler, Adam M., and Thomas J. Holt. "Patrol Officers' Perceived Role in Responding to Cybercrime." *Policing:* 35, no. 1 (March 2012): 165–81. https://doi.org/10.1108/13639511211215504.

Brundage, Miles. "Limitations and Risks of Machine Ethics." *Journal of Experimental & Theoretical Artificial Intelligence* 26, no. 3 (September 2014): 355–72. https://doi.org/10.1080/0952813X.2014.895108.

Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, et al. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Oxford: University of Oxford, February 2018. http://arxiv.org/abs/1802.07228.

Brynjolfsson, Erik, and Andrew Mcafee. "The Business of Artificial Intelligence: What It Can—and Cannot—Do for Your Organization." *Harvard Business Review*, July 2017.

———. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York London: W.W. Norton & Company, 2016. Kindle.

Bullee, Jan-Willem, Lorena Montoya, Marianne Junger, and Pieter Hartel. "Spear Phishing in Organisations Explained." *Information and Computer Security* 25, no. 5 (October 3, 2017): 593–613. https://doi.org/10.1108/ICS-03-2017-0009.

Bush, George. *The National Strategy to Secure Cyberspace*. Washington, DC: White House, 2003. https://www.hsdl.org/?view&did=1040.

Card, Orson Scott. *Ender's Game*. Rev. mass market ed. New York: Tor, 1994.

Caron, Christina. "Barack Obama's Favorite Book of 2018 Was 'Becoming.' Here's What Else He Liked." *New York Times*, December 31, 2018, https://www.nytimes.com/2018/12/28/arts/obama-favorites-2018.html.

Chang, Weiping, Wingyan Chung, Hsinchun Chen, and Shihchieh Chou. "An International Perspective on Fighting Cybercrime." In *Intelligence and Security Informatics*, edited by Richard Miranda, Daniel D. Zeng, Chris Demchak, Jenny Schroeder, and Therani Madhusudan, 379–84. Berlin: Springer, 2003.

Choo, K.-K. R., and R. G. Smith. "Criminal Exploitation of Online Systems by Organised Crime Groups." *Asian Criminology* 3 (2008): 37–59.

Christin, Nicolas. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." In *Proceedings of the 22nd International Conference on the World Wide Web*, 213–224. New York: ACM, 2013. https://doi.org/10.1145/2488388.2488408.

Ciancaglini, Vincenzo, Marco Balduzzi, Max Goncharov, and Robert McArdle. *Deepweb and Cybercrime: It's Not All about TOR.* Cupertino, CA: Trend Micro, 2013. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf.

Citron, Danielle, and Robert Chesney. "Deepfakes and the New Disinformation War." *Foreign Affairs*, December 11, 2018. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

Cox, Joseph. "Mexico's Drug Cartels Love Social Media." *Vice* (blog), November 4, 2013. https://www.vice.com/en_us/article/znwv8w/mexicos-drug-cartels-are-using-the-Internet-to-get-up-to-mischief.

Creighton, Jolene. "The 'Father of Artificial Intelligence' Says Singularity Is 30 Years Away." Futurism. February 14, 2018. https://futurism.com/father-artificial-intelligence-singularity-decades-away.

Decary-Hetu, D., and L. Giommoni. "Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous." *Crime, Law and Social Change* 67, no. 1 (February 2017): 55–75. https://doi.org/10.1007/s10611-016-9644-4.

Demirkan, H., S. Earley, and R. R. Harmon. "Cognitive Computing." *IT Professional* 19, no. 4 (2017): 16–20. https://doi.org/10.1109/MITP.2017.3051332.

Department of Defense. *DoD Cybersecurity Strategy 2015*. Washington, DC: Department of Defense, April 17, 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Department of Homeland Security. "2015 Fusion Center Success Stories." September 4, 2015. https://www.dhs.gov/2015-fusion-center-success-stories.

———. "Intelligence and Analysis/Private Sector Engagement." July 30, 2018, https://www.dhs.gov/intelligence-and-analysis-private-sector-engagement.

Department of Justice. "Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers." May 2015. https://it.ojp.gov/GIST/178/Cyber-Integration-for-Fusion-Centers--An-Appendix-to-the-Baseline-Capabilities-for-State-and-Major-Urban-Area-Fusion-Centers.

———. "Reporting Computer, Internet-Related, or Intellectual Property Crime." Accessed July 29, 2018. https://www.justice.gov/criminal-ccips/reporting-computer-Internet-related-or-intellectual-property-crime.

Dhande, Meenal. "What Is the Difference between AI, Machine Learning and Deep Learning?" *Geospatial World* (blog), May 6, 2017. https://www.geospatialworld.net/blogs/difference-between-ai%EF%BB%BF-machine-learning-and-deep-learning/.

Domestic Security Alliance Council. "Front Page." Accessed February 21, 2019. https://www.dsac.gov/front-page.

Earley, Kelly. "What Is 'Deepfake' Porn and Why Is Scarlett Johansson Speaking Out about It?" Daily Edge. January 2, 2019. http://www.dailyedge.ie/why-scarlett-johansson-is-speaking-out-about-deepfake-porn-4419670-Jan2019/.

Eden, Amnon H., James H. Moor, Johnny H Soraker, and Eric Steinhart. *Singularity Hypotheses: A Scientific and Philosophical Assessment*. New York: Springer, 2012.

Eggers, William D. *Delivering on Digital: The Innovators and Technologies That Are Transforming Government*. New York: Rosetta Books, 2016. Kindle.

Eilenberg, Rose. "Beyond Deep Fakes: CMU Method Transfers Style from One Video to Another." *University Wire*, September 18, 2018. ProQuest.

Eubanks, Nick. "The True Cost of Cybercrime for Businesses." *Forbes*, July 13, 2017. https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#302a77694947.

European Network and Information Security Agency. *National Cyber Security Strategies*. Heraklion, Greece: ENISA, May 2012. https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.

European Union Agency for Law Enforcement Cooperation. *Internet Organized Crime Threat Assessment 2018*. The Hague: European Cybercrime Centre, 2018. https://www.europol.europa.eu/activities-services/main-reports/Internet-organised-crime-threat-assessment.

Farokhmanesh, Megan. "Is It Legal to Swap Someone's Face into Porn without Consent?" Verge. January 30, 2018. https://www.theverge.com/2018/1/30/16945494/deepfakes-porn-face-swap-legal.

Fawbert, Dave. "This Deepfake Mashup of Jennifer Lawrence and Steve Buscemi Is Utterly Terrifying." Short List. Accessed March 10, 2019. https://www.shortlist.com/tech/deepfake-mashup-jennifer-lawrence-steve-buscemi/379641.

Federal Bureau of Investigation. "National Cyber Investigative Joint Task Force." Accessed December 3, 2018. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

Feldman, Sue, and Hadley Reynolds. "A Definition and Some Thoughts." *KM World* 23, no. 10 (November/December 2014). http://www.kmworld.com/Articles/News/News-Analysis/Cognitive-computing-A-definition-and-some-thoughts-99956.aspx.

Finklea, Kristin M., and Catherine A. Theohary. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Washington, DC: Congressional Research Service, July 20, 2012.

Floridi, Luciano. "Artificial Intelligence, Deepfakes and a Future of Ectypes." *Philosophy & Technology* 31, no. 3 (September 2018): 317–21. https://doi.org/10.1007/s13347-018-0325-3.

Frakes, Randall, and William Wisher. *The Terminator*. New York: Bantam Books, 1985.

Gehl, Robert W. "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network." *New Media & Society* 18, no. 7 (August 2016): 1219–35. https://doi.org/10.1177/1461444814554900.

Gevorkian, Ani, and Jadzia Pierce. "IoT and AI Update: California Legislature Passes Bills on Internet of Things, Artificial Intelligence, and Chatbots." *National Law Review*, October 4, 2018. https://www.natlawreview.com/article/iot-and-ai-update-california-legislature-passes-bills-Internet-things-artificial.

Gibson, William. *Neuromancer*. New York: Penguin Books, 2016.

Goodall, Noah J. "Machine Ethics and Automated Vehicles." In *Road Vehicle Automation*, edited by Gereon Meyer and S. Beiker, 93–102. Cham, Switzerland: Springer, 2014. https://doi.org/10.1007/978-3-319-05990-7_9.

Goodman, Marc. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. New York: Anchor Books, 2016. Kindle.

Gotsch, Ted. "Epic Gives Administration Good Marks in Cybersecurity, Less So in Civil Liberties." *Cybersecurity Policy Report* (October 25, 2010). ProQuest.

Güera, David, and Edward J. Delp. "Deepfake Video Detection Using Recurrent Neural Networks." Paper presented at the 15th IEEE International Conference on Advanced Video and Signal Based, Auckland, New Zealand, November 27–30, 2018. https://doi.org/10.1109/AVSS.2018.8639163.

Guidett, Ray, Greg Demeter, Dean Baratta, Justin Wagner, Frank E. Rodgers, J. Michael Barrett, Gerard LaSalle, and John Rollins. *New Jersey State Police Practical Guide to Intelligence Led Policing* (New York: Manhattan Institute for Policy Research, September 2006), https://www.nj.gov/njsp/divorg/invest/pdf/njsp_ilpguide_010907.pdf.

Hawkins, Derek. "The Cybersecurity 202: Trump Administration Seeks to Project Tougher Stance in Cyberspace with New Strategy." *Washington Post*, September 21, 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/21/the-cybersecurity-202-trump-administration-seeks-to-project-tougher-stance-in-cyberspace-with-new-strategy/5ba3e85d1b326b7c8a8d158a/.

Heath-Ferguson, Rachael. "Offline 'Stranger' and Online Lurker: Methods for an Ethnography of Illicit Transactions on the Darknet." *Qualitative Research* 17, no. 6 (2017): 683–698. https://doi.org/10.1177/1468794117718894.

Her Majesty's Government. *National Cyber Security Strategy 2016–2021*. London: Stationery Office, November 1, 2016.

Hines, Andy. "Strategic Foresight: The State of the Art." *Futurist* 40, no. 5 (September 2006): 18–21. https://www.questia.com/magazine/1G1-150978061/strategic-foresight-the-state-of-the-art.

Holl, Daniel. "New U.S. Intelligence Strategy Focuses on Cyber Threats and Artificial Intelligence." *Epoch Times*, January 24, 2019. https://www.theepochtimes.com/new-us-intelligence-strategy-focuses-on-cyber-threats-and-artificial-intelligence_2778123.html.

Holt, Thomas J. "Regulating Cybercrime through Law Enforcement and Industry Mechanisms." *Annals of the American Academy of Political and Social Science* 679, no. 1 (September 2018): 140–57. https://doi.org/10.1177/0002716218783679.

Holt, Thomas J., and Adam M. Bossler. "Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments." *CyberPsychology, Behavior & Social Networking* 15, no. 9 (September 2012): 464–72. https://doi.org/10.1089/cyber.2011.0625.

Horton, Christine. "Artificial Intelligence: Separating Hype from Reality." Channel Pro. January 12, 2018. https://www.channelpro.co.uk/advice/10702/artificial-intelligence-separating-hype-from-reality.

Hurlburt, George. “Shining Light on the Dark Web.” *Computer* 50, no. 4 (April 2017): 100–105. https://doi.org/10.1109/MC.2017.110.

Ingram, David. “Trump’s Artificial Intelligence Order Lacks Funding but Not a Target—China.” NBC News. February 11, 2019. https://www.nbcnews.com/tech/tech-news/trump-s-artificial-intelligence-order-lacks-funding-not-target-china-n970406.

International Monetary Fund. “Report for Selected Countries and Subjects.” April 2018. https://www.imf.org/external/pubs/ft/weo/2018/02/weodata/index.aspx.

INTERPOL. “The INTERPOL Global Complex for Innovation.” Accessed December 3, 2018. https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.

Itō, Jōichi, and Jeff Howe. *Whiplash: How to Survive Our Faster Future*. New York: Grand Central Publishing, 2016. Kindle.

Jerde, Ryan D. “Follow the Silk Road: How Internet Affordances Influence and Transform Crime and Law Enforcement.” Master’s thesis, Naval Postgraduate School, 2017.

Jewkes, Yvonne, and Majid Yar, eds. *Handbook of Internet Crime*. Cullompton, England: Willan Publishing, 2010.

Johnson, Clay, III. “Safeguarding against and Responding to the Breach of Personally Identifiable Information.” OMB Memorandum M-07-16. Washington, DC: Office of Management and Budget, May 22, 2007. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf.

Jones, M. Tim. “A Beginner’s Guide to Artificial Intelligence, Machine Learning, and Cognitive Computing.” *IBM Developer*, January 24, 2019. https://developer.ibm.com/articles/cc-beginner-guide-machine-learning-ai-cognitive/.

Joseph, Aghastise E. “Cybercrime Definition.” Computer Crime Research Center. Accessed August 26, 2018. http://www.crime-research.org/articles/joseph06/.

Kasparov, G. K., and Mig Greengard. *Deep Thinking: Where Machine Intelligence Ends and Human Creativity Begins*. 1st ed. New York: Public Affairs, 2017.

Kelley, Debbie. “Colorado Springs Middle-Schoolers Learn Drone Technology in New Flight and Space Class.” *Colorado Springs Gazette*, October 10, 2018. https://gazette.com/education/colorado-springs-middle-schoolers-learn-drone-technology-in-new-flight/article_66c9e6e4-cbf8-11e8-898c-27c046bb3b4a.html.

Kratsios, Michael. “Why the U.S. Needs a Strategy for AI.” *Wired*, February 11, 2019. https://www.wired.com/story/a-national-strategy-for-ai/.

Kroll, Justin. "Daisy Ridley to Star in Spy Movie 'A Woman of No Importance' for Paramount." *Variety*, January 24, 2017. https://variety.com/2017/film/news/daisy-ridley-a-woman-of-no-importance-paramount-1201968755/.

Kurzweil, Ray. "Ray Kurzweil on How We'll End up Merging with Our Technology." *New York Times*, March 14, 2017. https://www.nytimes.com/2017/03/14/books/review/thinking-machines-luke-dormehl.html.

Layton, Robert, and Paul A. Watters. *Automating Open Source Intelligence: Algorithms for OSINT*. Rockland, MA: William Andrew, 2015. ProQuest.

Magers, Jeffrey S. "CompStat: A New Paradigm for Policing or a Repudiation of Community Policing?" *Journal of Contemporary Criminal Justice* 20, no. 1 (February 2004): 70–79. https://doi.org/10.1177/1043986203262312.

Maras, Marie-Helen. "Inside Darknet: The Takedown of Silk Road." *Criminal Justice Matters* 98, no. 1 (October 2, 2014): 22–23. https://doi.org/10.1080/09627251.2014.984541.

Marcus, Gary. "Why We Should Think about the Threat of Artificial Intelligence." *New Yorker*, October 24, 2013. https://www.newyorker.com/tech/elements/why-we-should-think-about-the-threat-of-artificial-intelligence.

Markoff, John. "As Artificial Intelligence Evolves, so Does Its Criminal Potential." *New York Times*, October 23, 2016. https://www.nytimes.com/2016/10/24/technology/artificial-intelligence-evolves-with-its-criminal-potential.html.

Martin, James. "Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket.'" *Criminology & Criminal Justice* 14, no. 3 (July 1, 2014): 351–67. https://doi.org/10.1177/1748895813505234.

Masys, A. J. "Black Swans to Grey Swans: Revealing the Uncertainty." *Disaster Prevention and Management: An International Journal* 21, no. 3 (2012): 320–35. https://doi.org/10.1108/09653561211234507.

McAfee, Andrew, and Erik Brynjolfsson. *Machine, Platform, Crowd: Harnessing Our Digital Future*. New York: W. W. Norton & Company, 2017. Kindle.

Mckinnon, Andrew. *Hacking: Ultimate Hacking for Beginners, How to Hack*. Scotts Valley, CA: CreateSpace Independent Publishing, 2015.

Meserole, Chris, and Alina Polyakova. "The West Is Ill-Prepared for the Wave of 'Deep Fakes' That Artificial Intelligence Could Unleash." *Order from Chaos* (blog), May 25, 2018. https://www.brookings.edu/blog/order-from-chaos/2018/05/25/the-west-is-ill-prepared-for-the-wave-of-deep-fakes-that-artificial-intelligence-could-unleash/.

Mitnick, Kevin D. "Are You the Weak Link?" *Harvard Business Review* 81, no. 4 (April 2003): 18–20. EBSCO.

Mitnick, Kevin D., and William L. Simon. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. 1st ed. New York: Little, Brown and Company, 2011.

Modha, Dharmendra S., Rajagopal Ananthanarayanan, Steven K. Esser, Anthony Ndirango, Anthony J. Sherbondy, and Raghavendra Singh. "Cognitive Computing." *Communications of the ACM* 54, no. 8 (August 2011): 62–71. https://doi.org/10.1145/1978542.1978559.

Morag, Nadav. *Comparative Homeland Security: Global Lessons*. 2nd ed. Hoboken, NJ: John Wiley & Sons, 2018.

Morgan, Lisa. "How to Achieve Ethical Design." *Software Development Times*, November 5, 2018. https://sdtimes.com/ai/how-to-achieve-ethical-design/.

Morris, Tim. "Making Sense of Healthcare Data with AI to Improve Patient Care Outcomes." *Digital Health Age* (blog), February 19, 2019. http://digitalhealthage.com/making-sense-of-healthcare-data-with-ai-to-improve-patient-care-outcomes/.

Morselli, Carlo, and Katia Petit. "Law-Enforcement Disruption of a Drug Importation Network." *Global Crime* 8, no. 2 (May 2007): 109–30. https://doi.org/10.1080/17440570701362208.

National Council of ISACs. "Information Sharing and Analysis Centers (ISACs) and Their Roles in Critical Infrastructure Protection." January 2016. https://docs.wixstatic.com/ugd/416668_2e3fd9c55185490abcf2d7828abfc4ca.pdf.

———. "Member ISACs." Accessed October 14, 2018. https://www.nationalisacs.org/member-isacs.

National Crime Agency. "National Cyber Crime Unit." Accessed August 10, 2018. http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

National Cyber Security Centre. "About the NCSC." Accessed August 18, 2018. https://www.ncsc.gov.uk/information/about-ncsc.

National Fraud and Cyber Crime Reporting Centre. "What Is Action Fraud?" May 22, 2014. https://www.actionfraud.police.uk/what-is-action-fraud.

National Security Council. "Strategy to Combat Transnational Organized Crime: Definition." Obama White House. Accessed August 26, 2018. https://obamawhitehouse.archives.gov/node/60463.

Nicolescu, Basarab. "The Dark Side of Technological Singularity: New Barbarism," *Cybernetics & Human Knowing* 23, no. 4 (2016): 77–81. http://chkjournal.com/node/237.

Nilsson, Nils J. *Principles of Artificial Intelligence*. Palo Alto: Tioga, 1980.

Obama, Barack. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: White House, May 2011. https://www.hsdl.org/?abstract&did=5665.

Official website of Congressman Michael McCaul. "House Passes Critical Countering Drone Legislation in FAA." Press release. September 26, 2018. https://mccaul.house.gov/media-center/press-releases/house-passes-critical-countering-drone-legislation-in-faa.

Paquet-Clouston, Masarah, David Decary-Hetu, and Olivier Bilodeau. "Cybercrime Is Whose Responsibility? A Case Study of an Online Behaviour System in Crime." *Global Crime* 19, no. 1 (2018): 1–21. https://doi.org/10.1080/17440572.2017.1411807.

Persi Paoli, Giacomo, Judith Aldridge, Nathan Ryan, and Richard Warnes. *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR2091.html.

Peterson, Andrea, and Sean Pool. "Timeline: U.S. Cybersecurity Policy in Context; A Look at President Obama's Latest Executive Order and the Policies That Preceded It." Science Progress. February 13, 2013. https://scienceprogress.org/2013/02/u-s-cybersecurity-policy-in-context/.

Pistono, Federico, and Roman V. Yampolskiy. "Unethical Research: How to Create a Malevolent Artificial Intelligence." Paper presented at the Ethics for Artificial Intelligence Workshop, New York, NY, July 9–15, 2016. http://arxiv.org/abs/1605.02817.

Plesco, Ron, and Phyllis Schneck. "Criminal Public-Private Partnerships: Why Can't We Do That?" *Georgetown Journal of International Affairs* (Fall 2011): 151–54. ProQuest.

Police Executive Research Forum. *CompStat: Its Origins, Evolution, and Future in Law Enforcement Agencies*. Washington, DC: Bureau of Justice Assistance, 2013. https://www.bja.gov/publications/perf-compstat.pdf.

Poulsen, Kevin, and Eric Michael Summerer. *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. New York, Crown Publishing, 2015.

Public-Private Analytic Exchange Program. *AI: Using Standards to Mitigate Risk*. Washington, DC: Department of Homeland Security, 2018. https://www.dhs.gov/sites/default/files/publications/2018_AEP_Artificial_Intelligence.pdf.

Ralston, Bill, and Ian Wilson. *The Scenario-Planning Handbook: A Practitioner's Guide to Developing and Using Scenarios to Direct Strategy in Today's Uncertain Times*. Mason, OH: Thomson/South-Western, 2006.

Rathod, Digvijaysinh. "Darknet Forensics." *International Journal of Emerging Trends & Technology in Computer Science* 6, no. 4 (August 2017): 77–79.

Ranger, Steve. "Garry Kasparov Is Surprisingly Upbeat about Our Future AI Overlords." ZDNet. November 26, 2018. https://www.zdnet.com/article/garry-kasparov-is-surprisingly-upbeat-about-our-future-ai-overlords/.

Ratcliffe, Jerry. "Intelligence-Led Policing." *Trends & Issues in Crime and Criminal Justice*, no. 248 (April 2003): 1–6. https://aic.gov.au/publications/tandi/tandi248.

———. *Intelligence-Led Policing*. 2nd ed. New York: Routledge, 2016.

Reedy, Christianna. "Kurzweil Claims That the Singularity Will Happen by 2045." Futurism. October 5, 2017. https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045.

Revell, Timothy. "DeepMind AI Is Learning to Understand the 'Thoughts' of Others." *New Scientist*, February 28, 2018. https://www.newscientist.com/article/mg23731673-400-deepmind-ai-is-learning-to-understand-the-thoughts-of-others/.

Reynolds, Hadley, and Sue Feldman. "Cognitive Computing: Beyond the Hype." *KM World* 23, no. 7 (July/August 2014). http://www.kmworld.com/Articles/News/News-Analysis/Cognitive-computing-Beyond-the-hype-97685.aspx.

RFI. "France Has Most Cybercrime Victims in Europe." October 3, 2013. http://en.rfi.fr/economy/20131003-france-has-highest-cybercrime-rate-europe.

Rottman, Gabe. "Open Source Intelligence and Crime Prevention." *Free Future* (blog), December 21, 2012. https://www.aclu.org/blog/national-security/privacy-and-surveillance/open-source-intelligence-and-crime-prevention.

Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. 1st ed. New York: W. W. Norton & Company, 2018.

Security Asia. "Cybercriminals Adopting Advances in Artificial Intelligence, Warns Fortinet." November 24, 2017. https://www.networksasia.net/article/cybercriminals-adopting-advances-artificial-intelligence-warns-fortinet.1511493180.

Shipley, Todd G., and Art Bowker. *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*. Rockland, MA: William Andrew, 2013. ProQuest.

Simmons, Dan. *Hyperion*. London: Gollancz, 2011.

Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*. New York: Penguin Books, 2010.

Singer, P. W., and August Cole. *Ghost Fleet: A Novel of the Next World War*. Boston: Houghton Mifflin Harcourt, 2015.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014.

Sneed, Janine. "AI, Machine Learning and Deep Learning: Is There Really a Difference?" Medium. November 27, 2017. https://medium.com/cognitivebusiness/ai-machine-learning-and-deep-learning-is-there-really-a-difference-5631285052e4.

Spalevic, Zaklina, and Milos Ilic. "The Use of Dark Web for the Purpose of Illegal Activity Spreading." *Ekonomika* 63, no. 1 (March 2017): 73–82. http://dx.doi.org.libproxy.nps.edu/10.5937/ekonomika1701073S.

Stone, Peter, Russ Altman, Eric Horvitz, Deirdre Mulligan, Yoav Shoham, and Alan Mackworth. *Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence*. Stanford: Stanford University, September 2016. https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf.

Sui, Daniel, James Caverlee, and Dakota Rudesill. *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*. Washington, DC: Wilson Center, October 2015. https://www.wilsoncenter.org/sites/default/files/deep_web_report_october_2015.pdf.

Symantec Corporation. "Cybercrime Report 2011." November 2011. http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/assets/downloads/en-us/NCR-DataSheet.pdf.

Tadjdeh, Yasmin. "AI: A Tool for Good and Bad." *National Defense* 102, no. 774 (May 2018). ProQuest.

Techeblog. "Deepfake Technology Uses Artificial Intelligence to Superimpose Steve Buscemi onto Jennifer Lawrence in New Video." January 31, 2019. https://www.techeblog.com/deepfake-artificial-intelligence-steve-buscemi-jennifer-lawrence/.

Tegmark, Max. *Life 3.0: Being Human in the Age of Artificial Intelligence*. 1st ed. New York: Alfred A. Knopf, 2017.

———. *Life 3.0: Being Human in the Age of Artificial Intelligence*. 1st ed. New York: Alfred A. Knopf, 2017. Kindle.

Thalen, Mikael. "Jennifer Buscemi Is the Deepfake That Should Seriously Frighten You." Daily Dot. January 30, 2019. https://www.dailydot.com/debug/jennifer-buscemi-deepfake/.

Trump, Donald. "Executive Order on Maintaining American Leadership in Artificial Intelligence." February 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

———. *National Cyber Strategy of the United States of America*. Washington, DC: White House, September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Turing, Alan. "Lecture to the London Mathematical Society." Turing Digital Archive. February 20, 1947. http://www.turingarchive.org/viewer/?id=455&title=1.

Tuttle, Hilary. "Cybercrime Costs Businesses $11.7 Million Per Year." *Risk Management* 64, no. 10 (November 2017). ProQuest.

Verton, Dan. "Bush's Cybersecurity Plan Falls Short, Report Says." *Computerworld* 36, no. 52 (December 23, 2002). ProQuest.

Wadhwa, Amit, and Neerja Arora. "A Review on Cyber Crime: Major Threats and Solutions." *International Journal of Advanced Research in Computer Science* (2017): 2217–2221.

Walsh, William F. "CompStat: An Analysis of an Emerging Police Managerial Paradigm." *Policing: An International Journal* 24, no. 3 (2001): 347–62. https://doi.org/10.1108/13639510110401717.

Webpage of Robert W. Gehl. "About Robert W. Gehl." Accessed March 7, 2019. http://www.robertwgehl.org/index.php?styleSheetSelection=mobile.

Yonck, Richard. *Heart of the Machine: Our Future in a World of Artificial Emotional Intelligence*. 1st ed. New York: Arcade Publishing, 2017.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California