

Misty Blowers *Editor*

Evolution of Cyber Technologies and Operations to 2035

Advances in Information Security

Volume 63

Series editor

Sushil Jajodia, George Mason University, Fairfax, VA, USA

More information about this series at <http://www.springer.com/series/5576>

Misty Blowers
Editor

Evolution of Cyber Technologies and Operations to 2035



 Springer

Editor
Misty Blowers
Information Directorate
Air Force Research Laboratory
Rome, NY, USA

Advances in Information Security
ISBN 978-3-319-79505-8 ISBN 978-3-319-23585-1 (eBook)
DOI 10.1007/978-3-319-23585-1

Springer Cham Heidelberg New York Dordrecht London
© Springer International Publishing Switzerland 2015
Softcover reprint of the hardcover 1st edition 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

Evolution of Cyber Technologies and Operations to 2035 explores the future of cyber technologies and cyber operations which will influence advances in social media, cyber security, cyber physical systems, ethics, law, media, economics, infrastructure, military operations, and other elements of societal interaction in the upcoming decades. It provides a review of future disruptive technologies and innovations in cyber security. It informs military strategists about the future of cyber warfare and serves as an excellent reference for professionals and researchers working in the field of security, economics, law, and more. Students will also find this book useful as a reference guide or secondary textbook.

Written by leading experts in the field, authors explore specific examples of how future technical innovations vastly increase the interconnectivity of our physical and social systems and the growing need for resiliency in this vast and dynamic cyber infrastructure. In-depth coverage is provided on the future of social media, autonomy, stateless finance, quantum information systems, the Internet of Things, the dark web, space satellite operations, and global network connectivity along with the transformation of the legal and ethical considerations of these technologies in future military operations. The international nuances of cyber alliances, capabilities, and interoperability are confronted with a growing need for new laws, international oversight, and regulation.

Chapter 1 addresses the increasing need for resiliency of future cyber systems and technologies. It discusses how cyberspace defenders can maximize the flexibility of their systems by deliberately building in “inefficient” excess capacity, planning for and expecting failure, and creating personnel flexibility through training and exercises. The author also argues that defenders should reduce their attack surface by eliminating unnecessary capability in both hardware and software, resist users’ desire for continual rapid improvements in capability without adequate security testing, and segment their networks and systems into separate defended enclaves. Finally, the need for cyber defenders to position themselves to dynamically respond to attacks through improved situational awareness, effective cyberspace command

and control, and active defenses. This chapter shows how combining these approaches will enable the defenders of cyberspace systems to weather cyberspace attacks and spring upright after the passage of the storm.

Chapter 2 shows us how the “Internet of Things” (IoT) is poised to potentially change the way that human beings live their lives. This change will come about through the integration of billions of embedded devices and trillions of sensors into the world around us. These sensors will perceive the conditions around them and provide information to support an almost endless array of decision-supporting and decision-making capabilities. The effect of this capability will allow human beings to realize efficiencies in operation and slash costs in ways that would otherwise be impossible. IoT will be used to revolutionize our supply chains, manufacturing, infrastructure, transportation, clothing, homes, agriculture, and even our bodies. We will be able to instrument the world around us to the degree that we will increasingly rely on machines to augment and make decisions for us.

Chapter 3 discusses the convergence of cyber and electronic warfare. As nations embrace new and evolving communications networks, the reliance on these systems brings with it an implied vulnerability – the network itself. Understanding the current paradigm and accurately forecasting the future of communications will provide militaries with clear advantage in this facet of warfare. In this chapter we will examine the networks currently employed, their development, how they might look in the future, and finally how they relate to the overall electronic battlefield of the next several decades. Having an idea of how communication and operations will look in the future will help us craft the next generation of disruptive technologies for use during wartime.

Chapter 4 describes the relationships between the realm of cyber and space operations as they have been historically, are now, and as they will develop over the next 20 years. Space operations have long been critical for national security, providing intelligence, surveillance, and reconnaissance (ISR) capabilities from on high since the late 1950s. Predictably, American and international space assets have evolved exponentially since those early days, by now offering nations with navigation, timing, communications, weather, targeting, strategic warning, and defense abilities, among the more classical ISR roles. Both military and civilian affairs have been so enhanced by access to space that the realm has become indispensable to our day-to-day lives. However, the critical role of cyber relative to space operations is still somewhat hazy during normal space operations. Even with the dictum “You can’t have Space without Cyber” well known to space operators, understanding just how true that is and space systems’ vulnerabilities to cyber-attacks still needs to be fleshed out. To explore the aspects of cyber in space and cyber relative to space, this chapter will outline some of the current-generation systems, capabilities, and vulnerabilities and project what may be seen over the next 20 years from the view of space and cyber operators.

Chapter 5 discusses future trends in large data handling. From identifying prey in a distant landscape to today’s Big Data analytics, the task of information processing has been at the forefront of progress and will continue to be in future innovations. In the past, quantity of collected data was limited by our capability to transform it

into useful information. Factors such as low computing resources, minimal information storage, and small numbers of experienced analysts all constrained data collection by requiring careful feature and target selection. With the progression of Moore's law, rapid advance of storage technologies, cloud computing resources for hire, and distributed computing software, these constraints are relaxed. The result is an explosion in the amount of collected data from every imaginable sector of our lives. We discuss in this chapter the myriad fields in which large data analytics are being used, current and future challenges of this continued upward trend toward larger data collections, and future technology enablers in this field.

Chapter 6 presents an example of a specific visualization tool that may be used for a variety of big data problems. A specific problem is presented in which a cyberanalyst is inundated with vast amounts of data and tasked with identifying malicious network behavior. With a virtual reality (VR) head-mounted display, the display space for visualizing different information and data pertaining to cyber events becomes almost limitless. The head mounted VR display opens the door to new and innovative visualization techniques which enables a degree of spatial awareness that can be associated with information. The use of higher resolution and large panels enables analysts of the future to utilize more intuitive methods of sense-making in order to identify patterns of behavior within data making their jobs faster and easier and their information more reliable.

Chapter 7 provides an operational picture for the future use of quantum technologies. The author presents an alternative view of the future based on working quantum technologies and provides some past examples of disruptive technologies employed during WWII and technologies that rapidly developed during the 1980s. These examples highlight how the use of immature technologies can affect the strategic outcomes for war. The three phases of quantum technology development are discussed on a high level. The chapter closes on a fictional narrative to convey the perspective of an individual living in the 2025–2045 timeframe to illustrate how these quantum technologies may impact the world in that timeframe.

Chapter 8 explores the DarkNet and the future of underground networks. The future of the DarkNet is full of awe inspiring technological feats and dangers at the same time. We have been continuously plagued with technology that, from a security perspective, was not ready to be released to the general public. Knowledge of the DarkNet seems to be limited to IT professionals, hackers, and computer savvy criminals in modern times. However, more and more people are turning to this underground network as future generations become more connected and anonymity becomes an increasing concern. This is where the never-seen-before computer malware lives and thrives. You can find anything and everything known to man here, both legal and illegal (illegal drugs, weapons); even hitmen advertise in this part of the web. All of it can be conveniently delivered to your front door via UPS and FedEx. This chapter projects the dangers of the DarkNet and how underground networks may leverage it.

Chapter 9 takes an in-depth look into cryptocurrencies. Although most cryptocurrencies were created as a product of innovation in line with technological advances and with good intentions in mind, the use of such technologies by malicious

users is not a nuance concept. The author focuses her attention on the most common and popular of the cryptocurrencies, the Bitcoin. The Bitcoin has created a currency that can surpass institutions and eliminate transparency, providing a perfect agency. As governments grow concerned about taxation and their lack of control over the currency, Bitcoin also poses serious means of funding illicit activities and terrorist organizations. To what extent can Bitcoin develop and morph into a serious currency utilized to finance terrorism? This chapter explores how Bitcoin can manifest a credible security threat by directly changing systems of financial support. The first part of this chapter will describe how Bitcoin operates, including what features make it appealing to illicit networks and areas of vulnerabilities. The second part of this chapter will look at how Bitcoin is shaping terrorist financing, what the government response has been, and to what degree it has been effective. Finally the author will present a projection of the role of Bitcoins in the coming future.

Chapter 10 explores the current role of social media and its projected evolution. The rise in popularity of social media in protests and revolution in the present age presents a host of possibilities in the coming decades. The exploding use of social media is staggering, and the ability for populations and governments to stay connected is unprecedented. It is the author's position that basic human psychology and habit patterns observed today will greatly inform our understanding of how social media will be used in the future. The author explores two recent protests where social media played a significant role in the way the protests unfolded and concluded. It is to the reader to determine social media's ultimate effect on social protests, but consider the effect of social media to foment peace or violent and organize the demonstration and the ability of government to coordinate a response. These examples lead the author to make loose projections on the future of social media and its global impact on society.

Chapter 11 discusses the rules for autonomous cyber capabilities. It discusses how our capability to unleash autonomous systems into the wild on our behalf outpaces the degree to which we have pondered and resolved the myriad legal questions that arise. For instance, who is responsible if something goes wrong? Can responsibility even be determined? What rules should apply? What laws govern? Should autonomous cyber responses be allowed at all? This chapter outlines some of the key questions in this regard and seeks to explore these questions in light of the developing law for other autonomous systems. It will discuss the aspects that make cyber unique and propose rules that address such distinctions.

Chapter 12 is about ethical considerations in the cyber domain in future years. Defining proper ethical behavior in the cyber domain and making sure all societies and governments agree on cyber ethics will be an increasingly difficult challenge. Under current circumstances, democratic nations could be willing to reach bilateral agreements, but other nations might not be so cooperative. Cyber society is defined in this chapter as a combination of legislative actions, state and non-state actors, the military, and public-private partnerships. The difficulties in establishing a set of standards from geographically separate and ideologically diverse worldviews are presented, as well as discussions on critical infrastructure protections in both the public and private sectors. Finally, the chapter presents ethical considerations for state and non-state actors.

Chapter 13 is about the ethical challenges of state-sponsored hacktivism and the advent of “soft” war in which warfare tactics rely on measures other than kinetic force or conventional armed conflict to achieve the political goals and national interests. The author presents a brief history of cyber conflict and malevolent activities in the cyber domain. He then discusses the rise of state-sponsored hacktivism and the subsequent advent of state-sponsored internet activism. The soft war leads to “soft” law which calls moral guidelines and ethics into consideration in which the legal framework may not suffice to provide reliable guidance. Alternatively, best practices emerge from the shared practices of the interested parties and reflect their shared experience and shared objectives.

Chapter 14 is a collection of short essays written from the perspective of a younger generation – current high school students. The graduating classes of 2015–2016 have grown up fully immersed in this technological world and have a unique perspective on how we as humans will have to continue to adapt to it. The students’ task was to talk about “disruptive technologies” and how they see technology affecting our world in the year 2035. Various topics were selected such as cyber warfare, commercial and personal space travel, quantum computing, holographic enabling technologies, solar roads, and flying cars.

This book was designed to bring some of the most inquisitive, enlightened, and educated minds together to help us all understand the landscape of future cyber operations and societal concerns. We hope that the reader finds inspiration from reading this book to address some of the ethical concerns presented, to innovate new solutions to help shape a new world of interconnected devices and people, and to educate the next generation of scientist and engineers who will design technologies we could not even conceive of when writing this book.

This book could not have been made possible without the generous time commitment and passion of the authors whose ideas and insights are contained within to share with the world. In addition, I would like to express my most sincere gratitude both to the publisher and to a team of contributing technical reviewers who gave their time to ensure accuracy of technical content. Members of this team included the following:

1st Lieutenant Daniel Stambovsky, US Air Force
Captain Jon Williams, US Air Force
Mr. Jason Moore, US Air Force
Mr. Phil Zaleski, Exelis Inc.
Mr. Anthony Wong, Invincea Inc.

Thank you to all!

New York, NY

Misty Blowers

Contents

Cyberspace Resiliency: Springing Back with the Bamboo	1
William Bryant	
Internet of Things	19
David Fletcher	
The Invisible War: The Convergence of Cyber and Electronic Warfare	33
Gus Anderson and Lt Col Mark Hadley	
Cyber in Space: 2035	39
Capt Neil F. Bockus	
Future Trends in Large Data Handling	59
Hiren Patel	
The Application of Virtual Reality for Cyber Information Visualization and Investigation	71
Garrett Payer and Lee Trossbach	
Quantum Information Science	91
E. Thoreson	
Dark Web and the Rise of Underground Networks	107
Tim Singletary	
The Bitcoin: The Currency of the Future, Fuel of Terror	127
Anais Carmona	
The Rise of Social Media and Its Role in Future Protests and Revolutions	137
Paul Klensch Rozumski	
Is Skynet the Answer? Rules for Autonomous Cyber Response Capabilities	151
Capt Jarrod H. Stuard and James McGhee	

Ethical Considerations in the Cyber Domain..... 163
Justin M. Hubman, Zachary B. Doyle, Robert L. Payne III,
Thomas F. Woodburn, Branden G. McDaniel, and Joseph V. Giordano

**Ethical Challenges of ‘Disruptive Innovation’: State Sponsored
Hactivism and ‘Soft’ War**..... 175
George Lucas

**High School Student Vision: Disruptive Technologies – A Collection
of Works from a 2015–2016 High School Class**..... 185
Dan Scott, Rose Collins, Ryleigh Peterson, Liz Adams, Kyler Harrington,
Eoin Gallagher, Will Fruce, Chris Bedigian, Eve Kyle, Sophia Klemenz,
and Dana Tuohey

Advances in Inform

Misty Blowers Editor

Evolution of Cyber

Biblioteka Główna
Akademii Sztuki Wojennej

26652/III (CB)



03-026652-000-0

Computer Science

ISBN 978-3-319-79505-8

9 "783319"795058"

▶ springer.com

