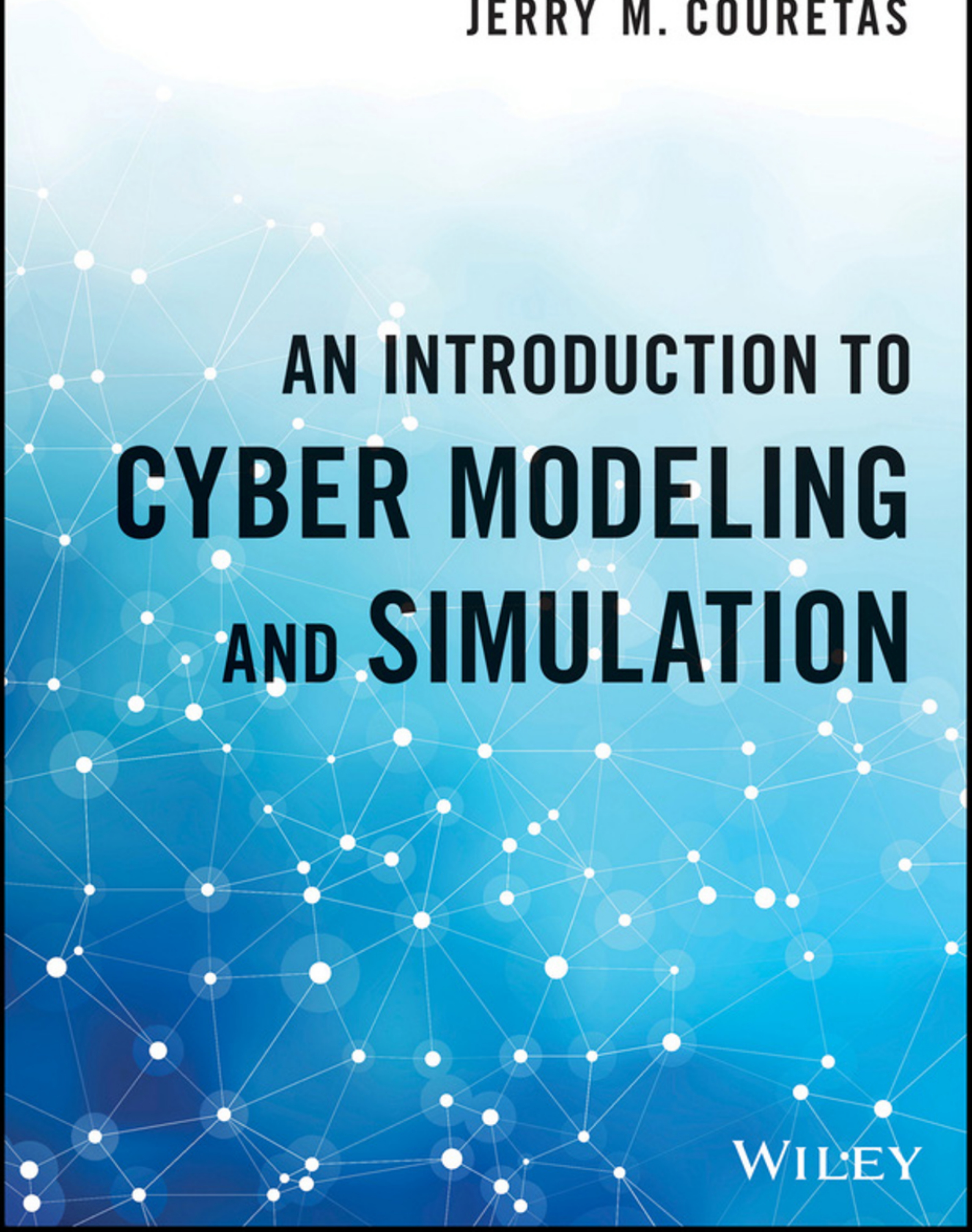
Wiley Series in Modeling and Simulation

JERRY M. COURETAS

AN INTRODUCTION TO CYBER MODELING AND SIMULATION



WILEY

An Introduction to Cyber Modeling and Simulation

Wiley Series in Modeling and Simulation

The Wiley Series in Modeling and Simulation provides an interdisciplinary and global approach to the numerous real-world applications of modeling and simulation (M&S) that are vital to business professionals, researchers, policymakers, program managers, and academics alike. Written by recognized international experts in the field, the books present the best practices in the applications of M&S as well as bridge the gap between innovative and scientifically sound approaches to solving real-world problems and the underlying technical language of M&S research. The series successfully expands the way readers view and approach problem solving in addition to the design, implementation, and evaluation of interventions to change behavior. Featuring broad coverage of theory, concepts, and approaches along with clear, intuitive, and insightful illustrations of the applications, the Series contains books within five main topical areas: Public and Population Health; Training and Education; Operations Research, Logistics, Supply Chains, and Transportation; Homeland Security, Emergency Management, and Risk Analysis; and Interoperability, Composability, and Formalism.

Spatial Agent-Based Simulation Modeling in Public Health: Design, Implementation, and Applications for Malaria Epidemiology
by *S. M. Niaz Arifin, Gregory R. Madey, Frank H. Collins*
The Digital Patient: Advancing Healthcare, Research, and Education
by *C. D. Combs (Editor), John A. Sokolowski (Editor), Catherine M. Banks (Editor)*

An Introduction to Cyber Modeling and Simulation

Jerry M. Couretas

WILEY

This edition first published 2019

Registered Office
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

Editorial Office
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Limit of Liability/Disclaimer of Warranty
The publisher and the authors make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties; including without limitation any implied warranties of fitness for a particular purpose. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for every situation. In view of on-going research, equipment modifications, changes in governmental regulations, and the constant flow of information relating to the use of experimental reagents, equipment, and devices, the reader is urged to review and evaluate the information provided in the package insert or instructions for each chemical, piece of equipment, reagent, or device for, among other things, any changes in the instructions or indication of usage and for added warnings and precautions. The fact that an organization or website is referred to in this work as a citation and/or potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this works was written and when it is read. No warranty may be created or extended by any promotional statements for this work. Neither the publisher nor the author shall be liable for any damages arising here from.

Library of Congress Cataloging-in-Publication Data

Names: Couretas, Jerry M., 1966– author.
Title: An introduction to cyber modeling and simulation / Jerry M. Couretas.
Description: Hoboken, NJ : John Wiley & Sons, 2019. | Series: Wiley series in
modeling and simulation | Includes bibliographical references and index. |
Identifiers: LCCN 2018023900 (print) | LCCN 2018036433 (ebook) |
ISBN 9781119420811 (Adobe PDF) | ISBN 9781119420835 (ePub) |
ISBN 9781119420873 (hardcover)
Subjects: LCSH: Computer simulation. | Computer security. | Cyberinfrastructure.
Classification: LCC QA76.9.C65 (ebook) | LCC QA76.9.C65 C694 2018 (print) |
DDC 005.8–dc23
LC record available at https://lccn.loc.gov/2018023900

Cover Design: Wiley
Cover Image: © MimaCZ/Getty Images

Set in 10/12pt Warnock by SPi Global, Pondicherry, India

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Dedication

This book is dedicated to Monica, Sophie, and Ella, for the time and patience that they provided to bring this work to fruition. I would also like to thank Jorge and Aida Carpio, for their support and mentoring. Finally, to my parents, Gus and Mary, for providing an example of persistence and faith.

Professionally, I would like to thank Mr. Rick Stotts for introducing me to modern cyber, Professor Bernard Zeigler, for his ongoing support from my student days to the present.

Contents

1

Brief Review of Cyber Incidents

> *When it comes to national security, I think this [i.e., cyber warfare] represents the battleground for the future. I've often said that I think the potential for the next Pearl Harbor could very well be a cyber-attack. If you have a cyber-attack that brings down our power grid system, brings down our financial systems, brings down our government systems, you could paralyze this country.*[1]
>
> Leon Panetta

The 1988 Morris Worm, designed to estimate the size of the Internet, caused the shutting down of thousands of machines and resulted in the Defense Advanced Research Projects Agency (DARPA) funding the first Computer Emergency Response Team (CERT) at Carnegie Mellon University (CMU). As shown in Table 1.1, cyberattacks have continued since 1988, with effects that range from data collection to controlling critical infrastructure.

Table 1.1 also provides a mix of documented cyber incidents, with only the Morris Worm in question, as to malevolent intent. Due to the multiple actors and actions, involving cyberattacks, a conversation around "resilience" (e.g. NIST Cybersecurity Framework) provides a means for communicating about how the overall system will continue to perform, in the face of adversity. In addition, resilience frames the discussion about an organization's operational risk; due to cyber, in this case. More specifically, the resilience view provides a means to organize the challenges associated with measuring and quantifying the broad scope of an organization's cyberattack surface by:

1) Recognizing that the autonomy and efficiencies that information systems provide are too valuable to forego, even if the underlying technologies provide a potential threat to business operations.

[1] "Cybersecurity 'battleground of the future,'" *United Press International,* 10 February 2011, available at http://www.upi.com/Top_News/US/2011/02/10/Cybersecurity-battleground-of-thefuture/UPI-62911297371939/, accessed on 10 January 2012.

An Introduction to Cyber Modeling and Simulation, First Edition. Jerry M. Couretas.

Table 1.1 Select cyber incidents.

Year	Cyberattack	Objective	Effects
1988	Morris Worm	Understand the number of hosts connected to the Internet	Removed thousands of computers from operation
2003	Slammer Worm	Denial of service	Disabled Ohio's Davis–Besse nuclear power plant safety monitoring system for nearly 5 h
2008	Conficker	Implant malware on target machines	Control target machines
2010	STUXNET	Take control of Siemens industrial control systems (ICS')	Destroyed centrifuges used for Iranian nuclear program
2012	Saudi Aramco (oil provider) business systems (aka Al Shamoon)	Wipe disks on Microsoft Windows-based systems	Destroyed ARAMCO business systems to cause financial losses due to their inability to bill customers for oil shipments
2013	South Korean Banks	"DarkSeoul" virus used to deny service and destroy data	Destroyed hard drives of selected business systems
	US Banks	Distributed Denial of Service (DDoS)	Caused financial losses through banks' inability to serve customers
	Rye Dam (NY)	Access control gates for opening and closing at will	Controlled dam gate system
2014	Sony Pictures	Data breach	Downloaded a large amount of data and posted it on the Internet; 3 wk before the release of a satirical film about North Korea
2015	Office of Personnel Management (OPM) breach	Gain access to information on US Government Personnel	Downloaded over 21 million US Government and contractor personnel files
2017	Equifax breach	Gain access to consumer credit information	Downloaded credit history and private information on over 143 million consumers

2) Understanding that cyber "security" (i.e. the ability to provide an effective deterrent to cyberattacks) is not achievable for most organizations in the short term, so resilience is one way to develop organizational policies and processes around
   a) mitigation scenarios for general cyberattacks
   b) comparing tacitly accepted cyber risk to business risks that we already transfer (e.g. hurricanes, earthquakes, natural disasters, etc.) to other organizations (e.g. insurance companies).
3) Coordinating the challenges associated with an organization's people being a key source of cyber vulnerability.

Resilience, therefore, provides an overarching approach, with some elements already modeled, for bundling the exposure associated with cyber and moving the discussion to a more manageable set of risks; analogous to operational challenges already mitigated or transferred through an organization's policies and processes. In addition, cyber risk management requires analytical evaluation and testable scenarios that enable contingency planning for each respective organization. Cyber risk assessment is a growing area of interest, and an inspiration for developing cyber modeling and simulation techniques.

1.1 Cyber's Emergence as an Issue

The issue of cyber security, somewhat slow to be recognized during information technology's rapid rate of development and dissemination into business enterprises over the last half century, often gets the same level of news coverage as natural disasters or stock market anomalies. While an Office of Personnel Management (OPM)[2] breach disclosing the private information of millions of US civil servants gets a few days of news, a new iPhone release will create weeks of chatter on social networks. Cyber insecurity is much less interesting to the general public than the Internet's entertainment and socialization prospects.

The same market growth for personal computing technologies, however, adds to unforeseen security challenges that networked technologies provide. Increased connectivity, often leading to tighter coupling (i.e. both technically and socially), challenges "open" information system architectures and their intended benefit. In addition, this increased connectivity provides, for the first time, an artificial domain, or space, through which nefarious actors can exercise potentially catastrophic effects. Cyber's ability to deny or manipulate entire regions of a state, at time constants much shorter than current management structures can handle, is a relatively recent realization. For example,

[2] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

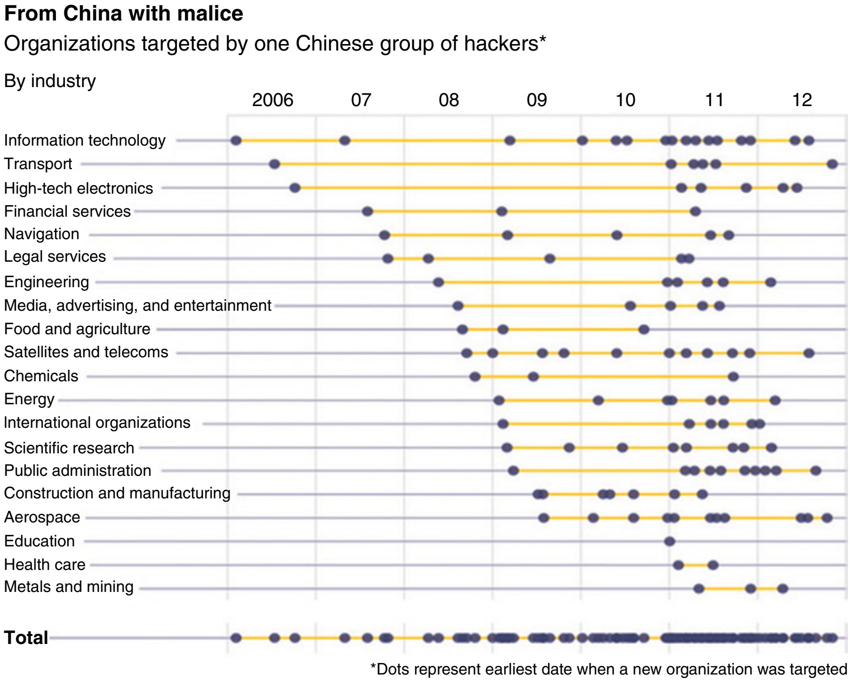


Figure 1.1 Organizations targeted by China. *Source:* Mandiant (2014), Fireeye https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

by 2015, reports (Frankel et al. 2015; Maynard and Beecroft 2015) on the potentially catastrophic nature of a cyberattack started to emerge. Along with the increasing importance of cyber, as a physical threat, there is an increased awareness, via news coverage (Figure 1.1).

In addition to Figure 1.1's profile of commercial cyber activity, military applications are expanding as well, with notable uses in Estonia and Georgia over the last decade.

1.2 Estonia and Georgia – Militarization of Cyber

For three weeks in 2007, the Republic of Estonia suffered a crippling cyberattack that left government, political, and economic facets of the country helpless (Yap 2009) (Figure 1.2).

This scenario provides a template to examine the policy, training, and technology options of a cyber-attacked state. Estonia's policy options were limited for a number of reasons, including:

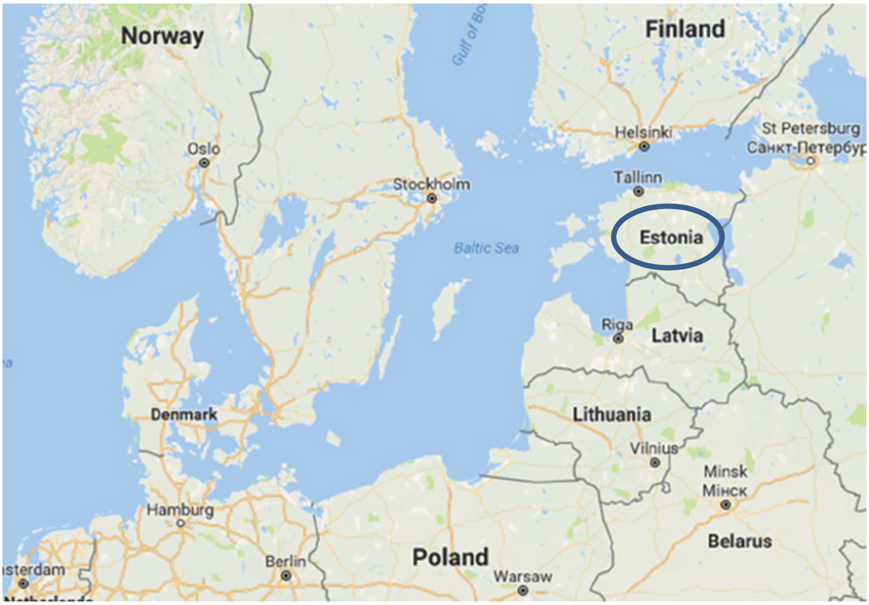


Figure 1.2 Map of N. Europe with Estonia (Google Maps).

- difficulty of attribution
- lack of international standards
- current political environment

Ultimately, unless a cyberattack causes indisputable damage, loss of human life, and can be traced back to a source with high certainty, it is unlikely that a state will conventionally respond in self-defense. Currently, there are no clear international laws,[3] or rules of engagement, that govern the rights of any sovereign state in the event of a cyberattack, without people dying or significant physical damage. The current approach is to take the existing laws and treaties and interpret them to fit cyber domain activities.

However, unlike a conventional attack, there are many more factors that blur the line in cyberspace. Attribution is usually spread across different sovereign states with limited physical evidence. Without a common, and agreed upon, definition of what constitutes a cyberattack, how can nations defend themselves without risking ethical, legal, and moral obligations? The fundamental dilemma a state faces is to balance its retaliatory options with the requisite legal justifications, if they cannot be confident of the source for the attack.

[3] The Tallinn Manual (https://ccdcoe.org/tallinn-manual.html) provides one approach for adapting laws of war to cyberspace.

While policy frameworks are still evolving to deal with cyber as a conflict domain, newly employed technologies provide unprecedented platforms for launching cyberattacks. For example, the major part of Estonia's assault suddenly stopped roughly a month after it began, suggesting that a botnet had been leased for the attacks. One Estonian official concluded that the attacks represented "a new form of public–private partnership" where the attacks were executed by organized crime, but directed by the Kremlin. "In Estonia," said then US National Security Agency chief General Keith Alexander, "all of a sudden we went from cybercrime to cyberwarfare."[4]

Some experts (Krepinevich 2012) believe the Estonia attack provided a way for Moscow to test its new technology, cyber weaponry, as a "proof of concept," in which the Russian Business Network (RBN) was given a target to show the Russian authorities how valuable cyber could be. In this way, the attacks on Estonia might be compared to how the Spanish Civil War provided a testing ground for German, Italian, and Soviet equipment and war-fighting concepts. While the evidence is circumstantial, it appears that just as Germany used its military's experience in Spain to assist in its development of the blitzkrieg form of warfare that it employed against Poland, the Low Countries, and France, shortly thereafter, the Russians used lessons learned from Estonia to better integrate cyber operations with traditional military operations in Georgia.

A year after the Estonia attacks, Georgia suffered the world's first mixed cyber–conventional attacks (Beidleman 2009). The cyberattacks were staged to kick off shortly before the initial Russian airstrikes as part of the Russian invasion in August 2008. The cyberattacks focused on government websites, with media, communications, banking, and transportation companies also targeted.

These botnet-driven DDoS attacks were accompanied by a cyber blockade that rerouted all Georgian Internet traffic through Russia and blocked electronic traffic in and out of Georgia. The impact of the cyberattacks on Georgia was significant, but less severe than the Estonia attacks since Georgia is a much less-advanced Internet society. Nonetheless, the attacks severely limited Georgia's ability to communicate its message to the world and its own people, and to shape international perception while fighting the war.

1.3 Conclusions

Modeling the broadly scoped set of systems that "cyber" currently covers, along with their associated effects, is a challenge without specifying the technical, process, or policy aspects of a scenario in question. While constructive modeling

[4] Keith B. Alexander, statement before the House Armed Services Committee, 23 September 2010, p. 4.

and simulation has made great contributions to describing the technical aspects of engineered systems for their testing and development, murky process and policy threads are still very much present in most cyber case studies – often providing the real security issues for the systems at risk. For example, computer technologies are often, simply, the implementation of processes for complex systems that support us. A “cyber” attack is really an attack on one of these processes we trust for our day-to-day business.

Cyber’s overarching use has implications across both a country’s business systems and its supporting civil infrastructure. Understanding the current state, in the cyber domain, therefore requires accurately assessing our systems and evaluating their maturity from a cyber standpoint. Using these assessments for defensive, or resiliency, analysis is the first step to verify M&S for cyber systems. Real-world cyber scenarios then use these assessments, as baselines, to represent both the scope and scale of networks with technologies and configurations that can easily span multiple generations of information technology.