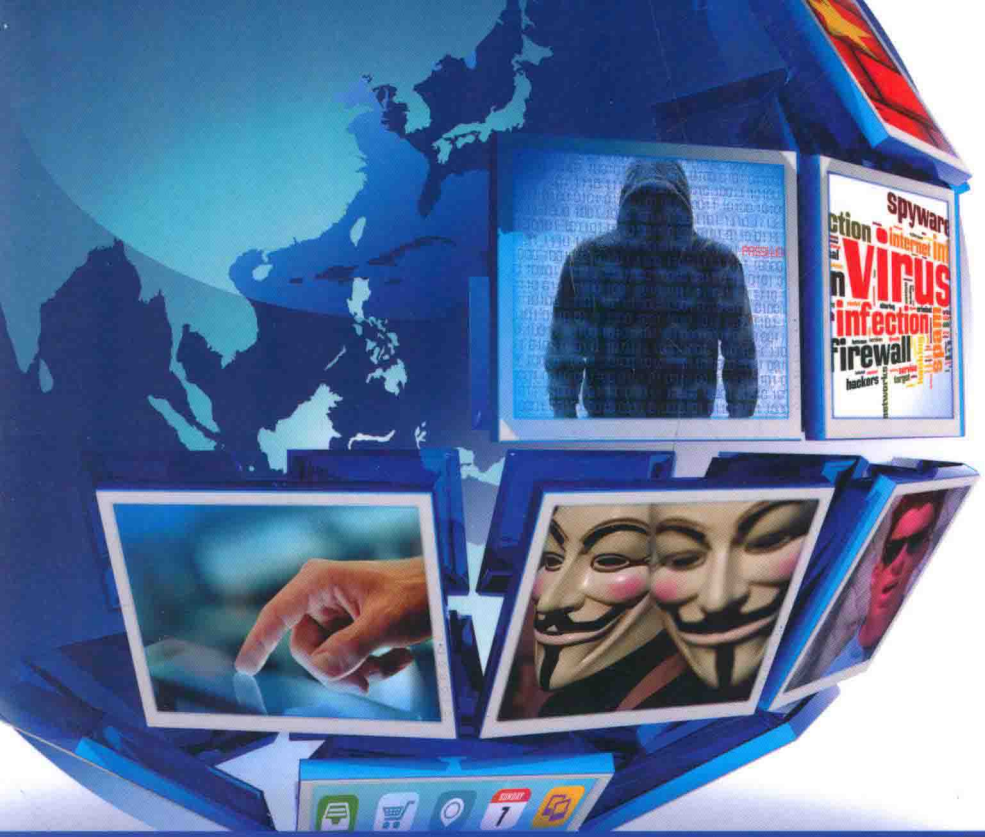

CYBERSECURITY AND CYBERWAR

WHAT EVERYONE NEEDS TO KNOW®

P.W. SINGER and ALLAN FRIEDMAN

CYBERSECURITY AND CYBERWAR

WHAT EVERYONE NEEDS TO KNOW®

P. W. SINGER AND
ALLAN FRIEDMAN

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trademark of Oxford University Press
in the UK and certain other countries.

"What Everyone Needs to Know" is a registered trademark of Oxford
University Press.

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016

Library of Congress Cataloging-in-Publication Data
Singer, P. W. (Peter Warren)
Cybersecurity and cyberwar : what everyone needs to know / Peter W. Singer,
Allan Friedman.
ISBN 978–0–19–991809–6 (hardback)—ISBN 978–0–19–991811–9 (paperback)
1. Computer security—United States 2. Computer networks—Security
measures—United States. 3. Cyberspace—Security measures—United States.
4. Cyberterrorism—United States—Prevention. 5. Information warfare—United
States—Prevention. I. Title.
QA76.9.A25S562 2014
005.8—dc23
2013028127

1 3 5 7 9 8 6 4 2
Printed in the United States of America
on acid-free paper

CYBERSECURITY AND CYBERWAR

WHAT EVERYONE NEEDS TO KNOW®

"In our digital age, the issues of cybersecurity are no longer just for the technology crowd; they matter to us all. Whether you work in business or politics, the military or the media—or are simply an ordinary citizen—this is an essential read."

—Eric Schmidt, Executive Chairman, Google

"This is the most approachable and readable book ever written on the cyber world. The authors have distilled the key facts and policy, provided sensible recommendations, and opened the debate generally to any informed citizen: a singular achievement. A must read for practitioners and scholars alike."

—Admiral James Stavridis, US Navy (Ret), former NATO Supreme Allied Commander

"In confronting the cybersecurity problem, it's important for all of us to become knowledgeable and involved. This book makes that possible—and also fascinating. It's everything you need to know about cybersecurity, wonderfully presented in a clear and smart way."

—Walter Isaacson, author of *Steve Jobs*

"If you read only one book about 'all this cyberstuff,' make it this one. Singer and Friedman know how to make even the most complicated material accessible and even entertaining, while at the same time making a powerful case for why *all* of us need to know more and think harder about the (cyber)world we know live in."

—Anne-Marie Slaughter, President, the New America Foundation

"Singer and Friedman blend a wonderfully easy to follow FAQ format with engaging prose, weaving explanations of the elements of cybersecurity with revealing anecdotes. From the fundamentals of Internet architecture to the topical intrigue of recent security leaks, this book provides an accessible and enjoyable analysis of the current cybersecurity landscape and what it could look like in the future."

—Jonathan Zittrain, Professor of Law and Professor of Computer Science at Harvard University, and author of *The Future of the Internet—And How to Stop It*

"Singer and Friedman do a highly credible job of documenting the present and likely future risky state of cyber-affairs. This is a clarion call."

—Vint Cerf, "Father of the Internet," Presidential Medal of Freedom winner

"I loved this book. Wow. Until I read this astonishing and important book, I didn't know how much I didn't know about the hidden world of cybersecurity and cyberwar. Singer and Friedman make comprehensible an impossibly complex subject, and expose the frightening truth of just how vulnerable we are. Understanding these often-invisible threats to our personal and national security is a necessary first step toward defending ourselves against them. This is an essential read."

—Howard Gordon, Executive Producer of *24* and co-creator of *Homeland*

CONTENTS

INTRODUCTION

Why Write a Book about Cybersecurity and Cyberwar?

"All this cyber stuff."

The setting was a Washington, DC, conference room. The speaker was a senior leader of the US Department of Defense. The topic was why he thought cybersecurity and cyberwar was so important. And yet, when he could only describe the problem as "all this cyber stuff," he unintentionally convinced us to write this book.

Both of us are in our thirties and yet still remember the first computers we used. For a five-year-old Allan, it was an early Apple Macintosh in his home in Pittsburgh. Its disk space was so limited that it could not even fit this book into its memory. For a seven-year-old Peter, it was a Commodore on display at a science museum in North Carolina. He took a class on how to "program," learning an entire new language for the sole purpose of making one of the most important inventions in the history of mankind print out a smiley face. It spun out of a spool printer, replete with the perforated paper strips on the side.

Three decades later, the centrality of computers to our lives is almost impossible to comprehend. Indeed, we are so surrounded by computers that we don't even think of them as "computers" anymore. We are woken by computerized clocks, take showers in water heated by a computer, drink coffee brewed in a computer, eat oatmeal heated up in a computer, then drive to work in a car controlled by hundreds of computers, while sneaking peeks at the last night's sport scores on a computer. And then at work, we spend most of our day pushing buttons on a computer, an experience so futuristic in

our parents' day that it was the stuff of *The Jetsons* (George Jetson's job was a "digital index operator"). Yet perhaps the best way to gain even a hint of computers' modern ubiquity is at the end of the day. Lie in bed, turn off the lights, and count the number of little red lights staring back at you.

These machines are not just omnipresent, they are connected. The computers we used as little kids stood alone, linked to nothing more than the wall electricity socket and maybe that spool printer. Just a generation ago, the Internet was little more than a link between a few university researchers. The first "electronic mail" was sent in 1971. The children of those scientists now live in a world where almost 40 trillion e-mails are sent a year. The first "website" was made in 1991. By 2013, there were over 30 trillion individual web pages.

Moreover, the Internet is no longer just about sending mail or compiling information: it now also handles everything from linking electrical plants to tracking purchases of Barbie dolls. Indeed, Cisco, a company that helps run much of the back end of the Internet, estimated that 8.7 billion devices were connected to the Internet by the end of 2012, a figure it believes will rise to 40 billion by 2020 as cars, fridges, medical devices, and gadgets not yet imagined or invented all link in. In short, domains that range from commerce to communication to the critical infrastructure that powers our modern-day civilization all operate on what has become a globalized network of networks.

But with the rise of "all this cyber stuff," this immensely important but incredibly short history of computers and the Internet has reached a defining point. Just as the upside of the cyber domain is rippling out into the physical domain, with rapid and often unexpected consequences, so too is the downside.

As we will explore, the astounding numbers behind "all this cyber stuff" drive home the scale and range of the threats: 97 percent of Fortune 500 companies have been hacked (and 3 percent likely have been too and just don't know it), and more than one hundred governments are gearing up to fight battles in the online domain. Alternatively, the problems can be conceptualized through the tough political issues that this "stuff" has already produced: scandals like WikiLeaks and NSA monitoring, new cyberweapons like Stuxnet, and the role that social networking plays in everything from the Arab Spring revolutions to your own concerns over personal privacy. Indeed, President Barack Obama declared that "cybersecurity risks pose some

of the most serious economic and national security challenges of the 21st century," a position that has been repeated by leaders in countries from Britain to China.

For all the hope and promise of the information age, ours is also a time of "cyber anxiety." In a survey of where the world was heading in the future, *Foreign Policy* magazine described the cyber area as the "single greatest emerging threat," while the *Boston Globe* claimed that future is already here: a "cyber world war" in progress that will culminate in "bloody, digital trench warfare."

These fears have coalesced into the massive booming business of cybersecurity, one of the fastest growing industries in the world. It has led to the creation of various new governmental offices and bureaucracies (the US Department of Homeland Security's National Cyber Security Division has doubled or tripled in size every year since its inception). The same is true for armed forces around the globe like the US Cyber Command and the Chinese "Information Security Base" (*xinxi baozhang jidi*), new military units whose very mission is to fight and win wars in cyberspace.

As we later consider, these aspects of "cyber stuff" raise very real risks, but how we perceive and respond to these risks may be even more crucial to the future, and not just of the Internet. As Joe Nye, the former Dean of the Harvard Kennedy School of Government, notes, if users begin to lose confidence in the safety and security of the Internet, they will retreat from cyberspace, trading "welfare in search of security."

Fears over cybersecurity increasingly compromise our notions of privacy and have allowed surveillance and Internet filtering to become more common and accepted at work, at home, and at the governmental level. Entire nations, too, are pulling back, which will undermine the economic and human rights benefits we've seen from global connectivity. China is already developing its own network of companies behind a "Great Firewall" to allow it to screen incoming messages and disconnect from the worldwide Internet if needed. As a Yale Law School article put it, all of these trends are "converging into a *perfect storm* that threatens traditional Internet values of openness, collaboration, innovation, limited governance and free exchange of ideas."

These issues will have consequences well beyond the Internet. There is a growing sense of vulnerability in the physical world from

new vectors of cyberattack via the virtual world. As a report entitled "The New Cyber Arms Race" describes, "In the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships."

Such a vision of costless war or instant defeat either scares or comforts, wholly dependent on which side of the cyberattack you're on. The reality, as we explore later in the book, is much more complex. Such visions don't just stoke fears and drive budgets. They also are potentially leading to the militarization of cyberspace itself. These visions threaten a domain that has delivered massive amounts of information, innovation, and prosperity to the wider planet, fuel tensions between nations, and, as the title of the aforementioned report reveals, maybe even have set in motion a new global arms race.

In short, no issue has emerged so rapidly in importance as cybersecurity. And yet there is no issue so poorly understood as this "cyber stuff."

Why Is There a Cybersecurity Knowledge Gap, and Why Does It Matter?

"Rarely has something been so important and so talked about with less and less clarity and less apparent understanding.... I have sat in *very* small group meetings in Washington... unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long term legal and policy implications of *any* decision we might make."

This is how General Michael Hayden, former Director of the CIA, described the cybersecurity knowledge gap and the dangers it presents. A major part of this disconnect is the consequence of those early experiences with computers, or rather the lack of them among too many leaders. Today's youth are "digital natives," having grown up in a world where computers have always existed and seem a natural feature. But the world is still mostly led by"digital immigrants,"

older generations for whom computers and all the issues the Internet age presents remain unnatural and often confusing.

To put it another way, few older than fifty will have gone through their university training even using a computer. Even the few who did likely used one that stood alone, not connected to the world. Our most senior leaders, now in their sixties and seventies, likely did not even become familiar with computers until well into their careers, and many still today have only the most limited experience with them. As late as 2001, the Director of the FBI did not have a computer in his office, while the US Secretary of Defense would have his assistant print out e-mails to him, write his response in pen, and then have the assistant type them back in. This sounds outlandish, except that a full decade later the Secretary of Homeland Security, in charge of protecting the nation from cyberthreats, told us at a 2012 conference, "Don't laugh, but I just don't use e-mail at all." It wasn't a fear of security, but that she just didn't believe e-mail useful. And in 2013, Justice Elena Kagan revealed the same was true of eight out of nine of the United States Supreme Court justices, the very people who would ultimately decide what was legal or not in this space.

It is not solely an issue of age. If it was, we could just wait until the old farts died off and all would be solved. Just because someone is young doesn't mean the person automatically has an understanding of the key issues. Cybersecurity is one of those areas that has been left to only the most technically inclined to worry their uncombed heads over. Anything related to the digital world of zeros and ones was an issue just for computer scientists and the IT help desk. Whenever they spoke, most of us would just keep quiet, nod our heads, and put on what author Mark Bowden calls "the glaze." This is the "unmistakable look of profound confusion and disinterest that takes hold whenever conversation turns to workings of a computer." The glaze is the face you put on when you can only call something "stuff." Similarly, those who are technically inclined too often roll their eyes at the foreign logic of the policy and business worlds, scoffing at the "old way" of doing business, without understanding the interactions between technology and people.

The result is that cybersecurity falls into a no man's land. The field is becoming crucial to areas as intimate as your privacy and as weighty as the future of world politics. But it is a domain only well known by "the IT Crowd." It touches every major area of

public- and private-sector concern, but only the young and the computer savvy are well engaged with it. In turn, the technical community that understands the workings too often sees the world only through a specific lens and can fail to appreciate the broader picture or nontechnical aspects. Critical issues are thus left misunderstood and often undebated.

The dangers are diverse and drove us in the writing of the book. Each of us, in whatever role we play in life, must make decisions about cybersecurity that will shape the future well beyond the world of computers. But often we do so without the proper tools. Basic terms and essential concepts that define what is possible and proper are being missed, or even worse, distorted. Past myth and future hype often weave together, obscuring what actually happened and where we really are now. Some threats are overblown and overreacted to, while others are ignored.

This gap has wide implications. One US general described to us how "understanding cyber is now a command responsibility," as it affects almost every part of modern war. And yet, as another general put it pointedly, "There is a real dearth of doctrine and policy in the world of cyberspace." His concern, as we explore later, was not just the military side needed to do a better job at "cyber calculus," but that the civilian side was not providing any coordination or guidance. Some liken today to the time before World War I, when the militaries of Europe planned to utilize new technologies like railroads. The problem was that they, and the civilian leaders and publics behind them didn't understand the technologies or their implications and so made uninformed decisions that inadvertently drove their nations into war. Others draw parallels to the early years of the Cold War. Nuclear weapons and the political dynamics they drove weren't well understood and, even worse, were largely left to specialists. The result was that notions we now laugh off as Dr. Strangelovian were actually taken seriously, nearly leaving the planet a radioactive hulk.

International relations are already becoming poisoned by this disconnect between what is understood and what is known. While we are both Americans, and thus many of the examples and lessons in this book reflect that background, the "cyber stuff" problem is not just an American concern. We were told the same by officials and experts from places ranging from China and Abu Dhabi to Britain

and France. In just one illustration of the global gap, the official assigned to be the "czar" for cybersecurity in Australia had never even heard of Tor, a critical technology to the field and its future (don't worry, you—and hopefully she—will learn what everyone needs to know about Tor in Part II).

This is worrisome not just because of the "naiveté" of such public officials, but because it is actually beginning to have a dangerous impact on global order. For instance, there is perhaps no other relationship as important to the future of global stability as that between the two great powers of the United States and China. Yet, as senior policymakers and general publics on both sides struggle to understand the cyber realm's basic dynamics and implications, the issue of cybersecurity is looming ever larger in US-China relations. Indeed, the Chinese Academy of Military Sciences released a report whose tone effectively captured how suspicion, hype, ignorance, and tension have all begun to mix together into a dangerous brew. "Of late, an Internet tornado has swept across the world...massively impacting and shocking the globe....Faced with this warm-up for an Internet war, every nation and military can't be passive but is making preparations to fight the Internet war."

This kind of language—which is mirrored in the US—doesn't illustrate the brewing global cyber anxiety. It also reveals how confusion and misinformation about the basics of the issue help drive that fear. While both sides, as we explore later on, are active in both cyber offense and defense, it is the very newness of the issue that is proving so difficult. Top American and Chinese governmental leaders talked with us about how they found cybersecurity to be far more challenging than the more traditional concerns between their nations. While they may not agree on issues like trade, human rights, and regional territorial disputes, they at least understand them. Not so for cyber, where they remain woefully ill-equipped even to talk about what their own nation is doing, let alone the other side. For example, a top US official involved in talks with China on cyber issues asked us what an "ISP" was (here again, don't fret if you don't yet know, we'll cover this soon!). If this had been back in the Cold War, that question would be akin to not knowing what an ICBM was in the midst of negotiating with the Soviets on nuclear issues.

Such matters are not just issues for generals or diplomats but also for all citizens. The general lack of understanding on this topic is becoming a democracy problem as well. As we write, there are some fifty cybersecurity bills under consideration in the US Congress, yet the issue is perceived as too complex to matter in the end to voters, and as a result, the elected representatives who will decide the issues on their behalf. This is one of the reasons that despite all these bills no substantive cybersecurity legislation was passed between 2002 and the writing of this book over a decade later.

Again, the technology has evolved so quickly that it is no surprise that most voters and their elected leaders are little engaged on cybersecurity concerns. But they should be. This field connects areas that range from the security of your bank accounts and online identity to broader issues of who in which governments can access your personal secrets and even when and where your nation goes to war. We are all users of this realm and are all shaped by it, yet we are not having any kind of decent public dialogue on it. "We're not having a really good, informed debate," as one professor at the US National Defense University put it. "Instead, we either punt the problem down the road for others to figure out, or to the small number of people who make important policy in the smoky backrooms." And even that is insufficient, given that most people in today's smoky backrooms have never been in an Internet chatroom.

How Did You Write the Book and What Do You Hope to Accomplish?

With all of these issues at play, the timing and value of a book that tried to tackle the basic issues that everyone should know about cybersecurity and cyberwar seemed ideal. And the format of this Oxford series, where all the books are in a "question and answer" style, seemed to hit that sweet spot.

As we set out to research and write the book, this question-and-answer style then structured our methodology. To put it another way, if you are locked into a Q and A format, you better first decide the right set of Qs.

We tried to gather all the key questions that people had about this field, not only those asked by people working in politics or technology, but also from our interactions and interviews well beyond. This set of questions was backed by what would have previously been called a "literature survey." In the old (pre-Internet) days, this meant