CYBERSECURITY AND CYBERWAR

WHAT EVERYONE NEEDS TO KNOW®

P.W. SINGER and ALLAN FRIEDMAN

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*

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

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

going to the library and pulling off the shelf all the books in that section of the Dewey decimal system. Today, on this topic especially, the sources range from books to online journals to microblogs. We were also greatly aided by a series of workshops and seminars at Brookings, the think tank in Washington we work at. These gathered key public- and private-sector experts to explore questions ranging from the efficacy of cyber deterrence to what can be done about botnets (all questions later dealt with in the book). We also held a series of meetings and interviews with key American officials and experts. They ranged from top folks like the Chairman of the Joint Chiefs, the highest-ranking US military officer, and the Director of the National Security Agency down to low-ranking systems administrators, from civilian governors, cabinet secretaries, and CEOs to small business owners and teenaged hackers. Our scope was global, and so the meetings also included leaders and experts from China (the foreign minister and generals from the PLA among them), as well as the UK, Canada, Germany, France, Australia, Estonia, United Arab Emirates, and Singapore. Finally, while it is a virtual world, we also visited key facilities and various cybersecurity hubs in locales that ranged from the DC Beltway and Silicon Valley to Paris and Abu Dhabi.

Over the course of this journey, we noticed a pattern. The questions (and the issues that came from them) generally fell under three categories. The first were questions of the essential contours and dynamics of cyberspace and cybersecurity, the "How does it all work?" questions. Think of these as the "driver's ed" part, which gives the basic building blocks to the online world. The second were questions on the broader implications of cybersecurity beyond cyberspace, the "Why does it matter?" questions. And then there were questions on the potential responses, the "What we can do?" questions. The following sections follow this basic structure.

And with the questions laid out, then came the task of answering them. This book is the result. While the questions are diverse, you'll notice that over the course of answering them, a few themes emerged to run through the book:

- *Knowledge matters*: It is vital we demystify this realm if we ever want to get anything effective done in securing it.
- *People matter*: Cybersecurity is one of those "wicked" problem areas that's rife with complexities and trade-offs. This is in

large part not because of the technical side, but because of the people part. The people behind the machines are inherently inside any problem or needed solution.
- *Incentives matter*: If you want to understand why something is or isn't happening in cyberspace, look to the motivations, the costs, and the tensions at play behind the issue. Indeed, anyone claiming a simple "silver bullet" solution in the cyber realm is either ignorant or up to no good.
- *The crowd matters*: This is not a realm where governments can or should have all the answers. Cybersecurity depends on all of us.
- *States matter*: That said, governments' roles are crucial, especially the United States and China. The reason is not just that these two nations remain powerful and influential, but that the interplay of their often differing visions of cybersecurity are critical to the future of both the Internet and world politics.
- *Cats matter*: In the end, the Internet is what we make of it. And that means while serious "stuff" is at play in it, cyberspace is also a fun, often whimsical realm, with memes like dancing babies and keyboard-playing cats. So any treatment of it should be sure to capture that whimsy.

To put it another way, our goal was to wrestle directly with the "cyber stuff" problem that set us on the journey. This is a book written by two researchers, following rigorous academic guidelines, and published by an esteemed university press. But our intent was not a book only for academics. The best research in the world is worthless if it does not find its way into the hands of those who need it. Indeed, the number of academic papers related to cybersecurity has increased at a compound annual growth rate of 20 percent for well over a decade. Yet no one would say that the broader world is all the more informed.

Instead, we embraced this series' core idea of "what everyone needs to know." Everyone does not need to know the software programming secrets of Stuxnet or the legal dynamics of ISP insurance schemes. But as we all become more engaged in and dependent on cybersecurity, there are certain building blocks of understanding that we all need to have. Ignorance is not bliss when it comes to cybersecurity. Cyber issues affect literally everyone: politicians wrestling

with everything from cybercrime to online freedom; generals protecting the nation from new forms of attack, while planning new cyberwars; business executives defending firms from once unimaginable threats, and looking to make money off of them; lawyers and ethicists building new frameworks for right and wrong. Most of all, cybersecurity issues affect us as individuals. We face new questions in everything from our rights and responsibilities as citizens of both the online and real world to how to protect ourselves and our families from a new type of danger.

So this is not a book only for experts, but rather a book intended to unlock the field, to raise the general level of expertise, and then push the discussion forward.

We hope that you find the journey useful, and ideally even enjoyable, just like the world of "cyber stuff" itself.

Peter Warren Singer and Allan A. Friedman,
August 2013, Washington, DC

Part I

HOW IT ALL WORKS

The World Wide What? Defining Cyberspace

"It's not a truck. It's a series of tubes."

This is how the late Alaska senator Ted Stevens famously explained cyberspace during a congressional hearing in 2006. As late-night humorist Jon Stewart noted, that someone who doesn't "seem to know jack BLEEP about computers or the Internet…is just the guy in charge of regulating it" is a near-perfect illustration of how disconnected Washington policymakers can be from technological realty.

While it's easy to mock the elderly senator's notion of electronic letters shooting through tubes, the reality is that defining ideas and terms in cyber issues can be difficult. Stevens's "tubes" is actually a mangling of the idea of "pipes," an analogy that is used by experts in the field to describe data connections.

If he wanted to be perfectly accurate, Stevens could have used science-fiction writer William Gibson's original conception of cyberspace. Gibson first used the word, an amalgam of "cybernetics" and "space," in a 1982 short story. He defined it two years later in his genre-revolutionizing novel *Neuromancer* as "A consensual hallucination experienced daily by billions of legitimate operators, in every nation.…A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data." Of course, if the senator had described cyberspace that way, most people would have thought him stoned rather than simply disconnected.

Part of why cyberspace is so difficult to define lies not only in its expansive, global nature, but also in the fact that the cyberspace of today is almost unrecognizable compared to its humble beginnings. The US Department of Defense can be considered the godfather of cyberspace, dating back to its funding of early computing and original networks like ARPANET (more on this soon). Yet even the Pentagon has struggled to keep pace as its baby has grown up. Over the years, it has issued at least twelve different definitions of what it thinks of as cyberspace. These range from the "notional environment in which digitized information is communicated over computer networks," which was rejected because it implied cyberspace was only for communication and largely imaginary, to a "domain characterized by the use of electronics and the electromagnetic spectrum," which was also rejected as it encompassed everything from computers and missiles to the light from the sun.

In its latest attempt in 2008, the Pentagon assembled a team of experts who took over a year to agree on yet another definition of cyberspace. This time they termed it "the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers." It is certainly a more detailed definition but so dense that one almost wishes we could go back to just the "tubes."

For the purposes of this book, we think it's best to keep it simple. At its essence, cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online. But rather than trying to find the exact perfectly worded definition of cyberspace, it is more useful to unpack what these definitions are trying to get at. What are the essential features that not only compose cyberspace, but also make it unique?

Cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared. This means that it is not merely a physical place and thus defies measurement in any kind of physical dimension.

But cyberspace isn't purely virtual. It comprises the computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computers, closed

intranets, cellular technologies, fiber-optic cables, and space-based communications.

While we often use "Internet" as shorthand for the digital world, cyberspace has also come to encompass the people behind those computers and how their connectivity has altered their society. One of the key features, then, of cyberspace is that its systems and technologies are man-made. As such, cyberspace is defined as much by the cognitive realm as by the physical or digital. Perceptions matter, and they inform cyberspace's internal structures in everything from how the names within cyberspace are assigned to who owns which parts of the infrastructure that powers and uses it.

This leads to an important point often misunderstood. Cyberspace may be global, but it is not "stateless" or a "global commons," both terms frequently used in government and media. Just as we humans have artificially divided our globe into territories that we call "nations" and, in turn, our human species into various groups like "nationalities," the same can be done with cyberspace. It relies on physical infrastructure and human users who are tied to geography, and thus is also subject to our human notions like sovereignty, nationality, and property. Or, to put it another way, cyberspace's divisions are as real as the meaningful, but also imaginary, lines that divide the United States from Canada or North from South Carolina.

But cyberspace, like life, is constantly evolving. The hybrid combination of technology and the humans that use it is always changing, inexorably altering everything from cyberspace's size and scale to the technical and political rules that seek to guide it. As one expert put it, "The geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch." The essential features remain the same, but the topography is in constant flux. The cyberspace of today is both the same as but also utterly different from the cyberspace of 1982.

The hardware and software that make up cyberspace, for instance, were originally designed for computers operating from fixed wires and telephone lines. Mobile devices were first the stuff of *Star Trek* and then only for the drug dealers on *Miami Vice* who could afford to have something as exotic as a "car phone." Today, a growing percentage of computing is moving onto mobile devices, so much so

that we've seen toddlers punch the screens of desktop computers as if they were broken iPads.

Along with the technology of cyberspace, our expectations of it are likewise evolving. This generates new norms of behavior, from how kids "play" to the even more powerful concept that we should all have access to cyberspace and be able to express our personal opinions within it, on everything from a Hollywood star's new hairdo to what we think of an authoritarian leader.

So what constitutes the Internet itself is evolving before us in an even more fundamental way. It is simultaneously becoming massively bigger (each day some 2,500,000,000,000,000,000 bytes are added to the global supply of digital information) and far more personalized. Rather than passively receiving this onslaught of online information, the individual users are creating and tailoring sites to their personal use, ultimately revealing more about themselves online. These sites range from social networks like Facebook in the United States and RenRen in China to microblogs like Twitter and the Chinese equivalents Tencent and Sina. Indeed, microblogs in China (called Weibo) have taken off to the extent that 550 million were registered in 2012.

Thus, while cyberspace was once just a realm of communication and then e-commerce (reaching over $10 trillion a year in sales), it has expanded to include what we call "critical infrastructure." These are the underlying sectors that run our modern-day civilization, ranging from agriculture and food distribution to banking, healthcare, transportation, water, and power. Each of these once stood apart but are now all bound together and linked into cyberspace via information technology, often through what are known as "supervisory control and data acquisition" or SCADA systems. These are the computer systems that monitor, adjust switching, and control other processes of critical infrastructure. Notably, the private sector controls roughly 90 percent of US critical infrastructure, and the firms behind it use cyberspace to, among other things, balance the levels of chlorination in your city's water, control the flow of gas that heats your home, and execute the financial transactions that keep currency prices stable.

Cyberspace is thus evolving from "the nervous system—the control system of our economy," as President George W. Bush once said, into something more. As *Wired* magazine editor Ben Hammersley

describes, cyberspace is becoming "the dominant platform for life in the 21st century."

> We can bitch about it, but Facebook, Twitter, Google and all the rest are, in many ways the very definition of modern life in the democratic west. For many, a functioning Internet with freedom of speech, and a good connection to the social networks of our choice is a sign not just of modernity, but of civilization itself. This is not because people are "addicted to the video screen," or have some other patronizing psychological diagnosis. But because the Internet is where we live. It's where we do business, where we meet, where we fall in love. It is the central platform for business, culture, and personal relationships. There's not much else left. To misunderstand the centrality of these services to today's society is to make a fundamental error. The Internet isn't a luxury addition to life; for most people, knowingly or not, it is life.

But just as in life, not everyone plays nice. The Internet that we've all grown to love and now need is increasingly becoming a place of risk and danger.

Where Did This "Cyber Stuff" Come from Anyway? A Short History of the Internet

"Lo."

This was the very first real word transmitted over the computer network that would evolve into the Internet. But rather than the beginning of some profound proclamation like "Lo and behold," "Lo" was instead the product of a system failure. In 1969, researchers at UCLA were trying to log into a computer at the Stanford Research Institute. But before they could type the "g" in the word "log," the computer at the Stanford end of the network crashed. However, the ARPANET project, so named as it was funded by the Advanced Research Projects Agency (ARPA), would eventually transform how computers shared data and, with that, everything else.

Electronic communication networks have been shaping how we share information since the invention of the telegraph, the device that some now look back on and call the "Victorian Internet." The hype around that old technology were similarly high; contemporaries declared that, with the telegraph, "It is impossible that old prejudices and hostilities should longer exist."

What makes the Internet distinct from prior communication networks like the old telegraphs and then telephone networks, however, is that it is packet-switched instead of circuit-switched. Packets are small digital envelopes of data. At the beginning of each packet, essentially the "outside" of the envelope, is the header, which contains details about the network source, destination, and some basic information about the packet contents. By breaking up flows of data into smaller components, each can be delivered in an independent and decentralized fashion, then reassembled at the endpoint. The network routes each packet as it arrives, a dynamic architecture that creates both flexibility and resiliency.

Packet-switching was not developed to allow the United States to maintain communications even in the event of a nuclear attack, a common myth. It was really just developed to better enable more reliable, more efficient connections between computers. Prior to its rise in the 1970s, communication between two computers required a dedicated circuit, or preassigned bandwidth. This direct link meant those resources could not be used by anyone else, even when no data was being transmitted. By breaking these conversations into smaller parts, packets from multiple distinct conversations could share the same network links. It also meant that if one of the network links between two machines went down mid-communication, a transmission could be automatically rerouted with no apparent loss of connection (since there was never a connection to begin with).

ARPA (now DARPA, with a D for "Defense" added) was an organization developed by the Pentagon to avoid technological surprise by leaping ahead in research. Computers were proliferating in the late 1960s, but even more researchers wanted to use them than was available. To ARPA, that meant finding ways to allow people at different institutions to take advantage of unused computer time around the country.

Rather than have dedicated—and expensive—connections between universities, the vision was a network of shared data links, sharing computational resources. Individual machines would each be connected with an Interface Message Processor that handled the actual network connection. This network was ARPANET, home of the first "Lo" and start of the modern cyber era. That first 1969 link from UCLA to Stanford grew to link forty nodes in 1972. Soon more universities and research centers around the world joined this first network, or alternatively created their own networks.

For the purposes of the modern Internet, a series of packets sent between machines on a single network does not count as an "internet." Internet implies connecting many different networks, in this case these various other computer networks beyond ARPANET that soon emerged but remained unlinked.

The challenge was that different networks used very different underlying technology. The technical problem boiled down to abstracting these differences and allowing efficient communication. In 1973, the solution was found. Vint Cerf, then a professor at Stanford, and Robert Khan of ARPA refined the idea of a common transmission protocol. This "protocol" established the expectations that each end of the communication link should make of the other. It began with the computer equivalent of a three-way handshake to establish a connection, continuing through how each party should break apart the messages to be reassembled, and how to control transmission speeds to automatically detect bandwidth availability.

The brilliance of the model is how it breaks the communication into "layers" and allows each layer to function independently. These packets, in turn, can be sent over any type of network, from sound waves to radio waves to light pulses on a glass fiber. Such Transport Control Protocols, or TCPs, could be used over all sorts of packet protocols, but we now use a type called the Internet Protocol, or IP, almost exclusively in the modern Internet.

This protocol enabled the creation of a network of networks. But, of course, the Internet didn't stop there. The new links excelled at connecting machines, but humans excel at making technology conform to their whims. As people shared machines for research, they started leaving messages for each other, simple files that could be

edited to form a conversation. This became clunky, and in 1972 Ray Tomlinson at the technical consulting firm BBN wrote a basic program to read, compose, and send messages. This was e-mail: the first Internet "killer app." Within a year, a majority of traffic across the network originally created for research was e-mail. Now networked communication was about people.

The last step in creating the modern Internet was eliminating barriers to entry. Early use was limited to those who had access to the networked computers at research and defense institutions. These organizations communicated via dedicated data lines. As the evident value of networked communication grew and the price of computers dropped, more organizations sought to join. Modems, which convert data to sound waves and back, allowed basic phone lines to serve as links to other computers.

Soon, researchers outside computer science wanted access, not just to take advantage of the shared computing resources, but also to study the new networking technology itself. The US National Science Foundation then connected the existing supercomputering centers around the country into the NSFnet, which grew so rapidly that the expansion required commercial management. Each upgrade brought greater demand, the need for more capacity, and independently organized infrastructure. The architecture of a "backbone" that managed traffic between the different regional networks emerged as the efficient solution.

This period also saw the introduction of the profit motive in Internet expansion. For instance, by this point Vint Cerf had joined the telecommunications firm MCI. In 1983, he led efforts to start MCI mail, the first commercial e-mail service on the Internet. By the late 1980s, it became obvious that managing the nascent Internet was not the business of the research community. Commercial actors could provide the necessary network services supporting the Internet and become avid consumers as well. So the White House Office of Science and Technology developed a plan to expand and commercialize the backbone services, seeing it as the only way that the new Internet could truly take off.

The planners envisioned a decade-long process, though, with the final stages of commercial handover not completed until the late 1990s. Fortunately, a young senator from Tennessee became convinced it should speed up. In 1989, Al Gore authored a bill calling

for quicker privatization of the network. While he would later make a slight overstatement that he "took the initiative in creating the Internet," this move by Congress to accelerate things was crucially important to the Internet's expansion. By the time Gore was Vice President in 1994, the NSF was turning over official control of regional backbone connections to private interests.

This privatization coincided with various new inventions and improvements that then democratized and popularized the Internet. In 1990, a researcher at the European research center CERN in Switzerland took a relatively obscure form of presenting information in a set of linked computer documents and built a new networking interface for it. With this HyperText Transfer Protocol (HTTP), and an accompanying system to identify the linked documents (URLs), Tim Berners-Lee "invented" the World Wide Web as we now look at it. Amusingly, when Berners-Lee tried to present it at an academic conference, his breakthrough wasn't considered worthy enough even to make a formal panel. Instead, he was relegated to showing a poster on it in a hallway. A few years later, researchers at the University of Illinois introduced the Mosaic web browser, which simplified both web design and introduced the new practice of "web surfing" for the general public.

And whether we like to admit it or not, this is the period when the pornography industry proved integral to the Internet's history. A darker domain that some estimate makes up 25 percent of all Internet searches, the smut industry drove both new online users and new online uses like instant messaging, chatrooms, online purchasing, streaming video, trading files, and webcams (and the growing demands each of these placed on bandwidth, driving more underlying business). "Of course pornography has played a key role in the Web," says Paul Saffo, an analyst with the Institute for the Future, a Silicon Valley think tank. "Porn is to new media formats what acne is to teenagers," he said. "It's just part of the process of growing up."

And soon the mainstream media started to wake up to the fact that something big was happening online. As the *New York Times* reported in 1994 (in a printed newspaper, of course!), "Increasing commercialization of the Internet will accelerate its transformation away from an esoteric communications system for American

computer scientists and into an international system for the flow of data, text, graphics, sound and video among businesses, their customers and their suppliers."

Lo and behold indeed.

How Does the Internet Actually Work?

For a few hours in February 2008, Pakistan held hostage all the world's cute cat videos.

The situation came about when the Pakistani government, in an attempt to prevent its own citizens from accessing what it decided was offensive content, ordered Pakistan Telecom to block access to the video-sharing website YouTube. To do so, Pakistan Telecom falsely informed its customers' computers that the most direct route to YouTube was through Pakistan Telecom and then prevented Pakistani users from reaching the genuine YouTube site. Unfortunately, the company's network shared this false claim of identity beyond its own network, and the false news of the most direct way to YouTube spread across the Internet's underlying mechanisms. Soon over two-thirds of all the world's Internet users were being misdirected to the fake YouTube location, which, in turn, overwhelmed Pakistan Telecom's own network.

The effects were temporary, but the incident underscores the importance of knowing how the Internet works. The best way to gain this understanding is to walk through how information gets from one place to another in the virtual world. It's a bit complex, but we'll do our best to make it easy.

Suppose you wanted to visit the informative and—dare we say—entertaining website of the Brookings Institution, the think tank where we work. In essence, you have asked your device to talk to a computer controlled by Brookings in Washington, DC. Your machine must learn where that computer is and establish a connection to enable communication.

The first thing your computer needs to know is how to find the servers that host the Brookings web page. To do that, it will use the Internet Protocol (IP) number that serves as the address for endpoints on the Internet. Your machine was most likely automatically assigned an IP address by your Internet service provider or

whatever network you are using. It also knows the address of its router, or the path to the broader Internet. Finally, your computer knows the address of a Domain Name System server.

The Domain Name System, or DNS, is the protocol and infrastructure through which computers connect domain names (human memorable names like Brookings.edu) to their corresponding IP addresses (machine data like 192.245.194.172). The DNS is global and decentralized. Its architecture can be thought of as a tree. The "root" of the tree serves as the orientation point for the Domain Name System. Above that are the top-level domains. These are the country codes such as .uk, as well as other domains like .com and .net. Each of these top-level domains is then subdivided. Many countries have specific second-level domains, such as co.uk and ac.uk, to denote business and academic institutions, respectively.

Entry into the club of top-level domains is controlled internationally through the Internet Corporation for Assigned Names and Numbers (ICANN), a private, nonprofit organization created in 1998 to run the various Internet administration and operations tasks that had previously been performed by US government organizations.

Each top-level domain is run by a registry that sets its own internal policies about domains. Organizations, such as Brookings or Apple or the US Department of State, acquire their domains through intermediaries called registrars. These registrars coordinate with each other to ensure the domain names in each top-level domain remain unique. In turn, each domain manages its own subdomains, such as mail.yahoo.com.

To reach the Brookings domain, your computer will query the DNS system through a series of resolvers. The basic idea is to go up the levels of the tree. Starting with the root, it will be pointed to the record for .edu, which is managed by Educause. Educause is the organization of some 2,000 educational institutions that maintains the list of every domain registered in .edu. From this list, your computer will then learn the specific IP address of Brookings's internal name server. This will allow it to address specific queries about content or applications from inside the Brookings domain. Then, the Brookings name server will direct your computer to the specific content it is looking for, by returning the IP address of the machine that hosts it.

In reality, this process is a little more complex. For example, servers often store data locally in caches for future use, so that every query does not have to go to the root, and the protocol includes specific error conditions to handle errors predictably. The rough outline above, however, gives a sense of how it all works.

Now that your computer has the location of the data, how will that data get to your computer? The server at Brookings needs to know that it should send data to your machine, and the data needs to get there. Figure 1.1 illustrates how your computer requests a web page by breaking down the request into packets and sending them across the Internet. First, at the "layer" of the application, your browser interprets the click of your mouse as a command in the HyperText Transfer Protocol (HTTP), which defines how to ask for and deliver content. This command is then passed down to the transport and network layers. Transport is responsible for breaking the data down into packet-sized chunks and making sure that all of

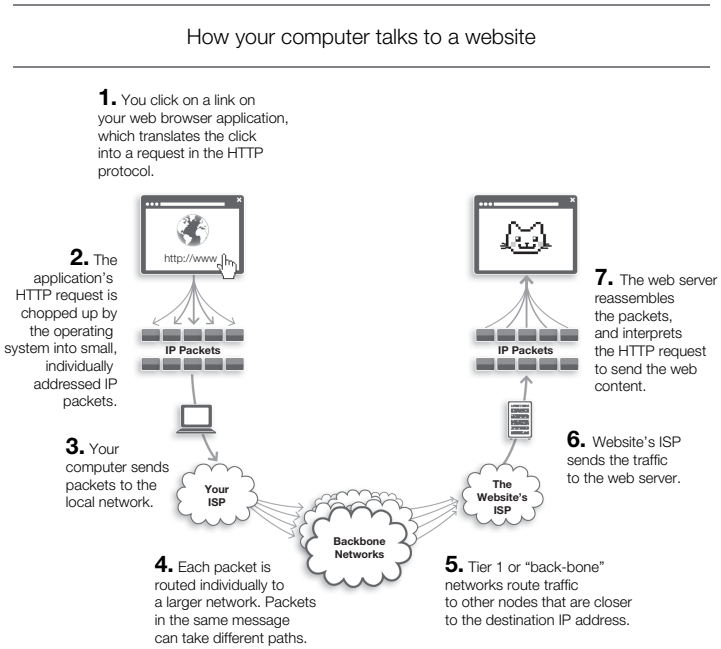

Figure 1.1