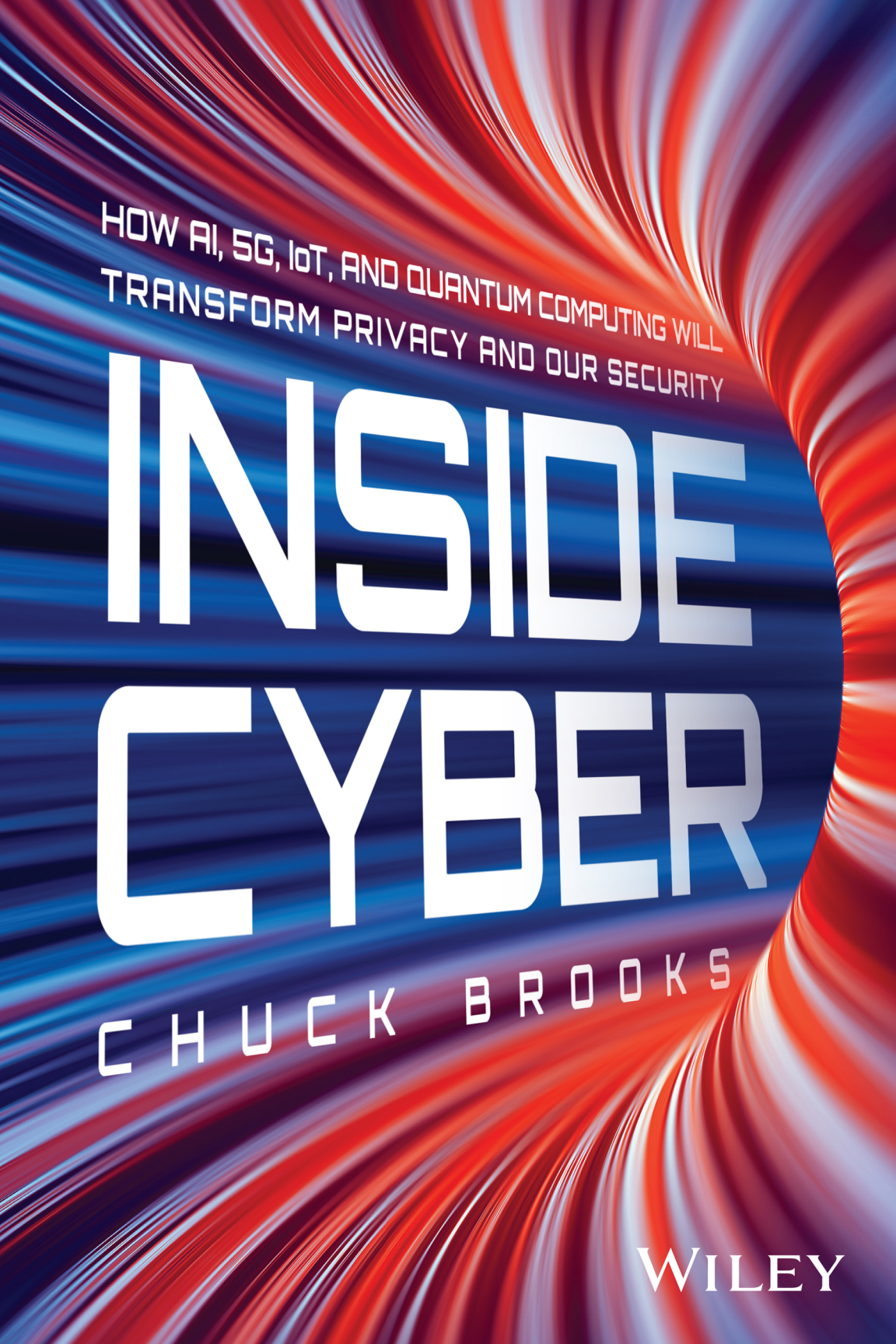
HOW AI, 5G, IoT, AND QUANTUM COMPUTING WILL TRANSFORM PRIVACY AND OUR SECURITY
INSIDE CYBER
CHUCK BROOKS
WILEY

HOW AI, 5G, IoT, AND QUANTUM COMPUTING WILL TRANSFORM PRIVACY AND OUR SECURITY

INSIDE CYBER

CHUCK BROOKS

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data is Available:

ISBN 9781394254941 (cloth)
ISBN 9781394254958 (epub)
ISBN 9781394254965 (epdf)

Cover Design: Wiley
Cover Image: © JuSun/Getty Images
Author Photo: Courtesy of the Author

I dedicate this book to my family: my wife, Mary;
daughters, Nina and Tanya; my sister, Joanne;
my in-laws, Bob and Marie;
and especially to my late parents, Dorothy and Norman.
They all have been a real source of inspiration and support for me.

Contents

Preface

My interest in science and technologies as they relate to security was spawned early in my career when I was a staffer for the late Senator Arlen Specter of Pennsylvania. In that role, I covered many security and foreign affairs issues and developed both a passion and expertise for the topics. Then came 9/11 and the world changed. Security and technologies became a top priority for the government, and I was recruited to become part of a start-up called the Department of Homeland Security, specifically with the newly formed Science & Technology Directorate. My focus was on technologies for CBRNE, (chemical biological, radiological, nuclear, and explosives). Cybersecurity, although in its early stages, was part of that threat matrix of technologies to explore.

After DHS, my career took me to the private sector where I continued my work pursuit in the cybersecurity and emerging technologies field. This included various executive roles at Xerox, Rapiscan, and General Dynamics. There is no substitute for real work experience in both government and industry.

In addition, I became a contributor to *Forbes*, and a visiting editor for *Homeland Security Today*. I became a prolific writer and my articles and comments appeared in the *Washington Post*, *Dark Reading*, *Skytop Media*, *GovCon*, *Security Info Watch*, *Barrons*, *The Hill*, *Federal Times*, and others on cybersecurity and emerging technology topics. I continue to write every week.

Then it was time to teach that knowledge and I added the fourth triad of academia to government, industry, and media: first at Johns Hopkins University where I taught a homeland security course, and subsequently for the past seven years at Georgetown University in their graduate cybersecurity and intelligence programs.

As I was researching the topics of emerging technologies on the horizon and their security implications for a graduate course I teach at Georgetown University's Cybersecurity Risk Management Program

called "Disruptive Technologies and Organizational Management," I started to see a pattern. Every week there appears to be a breakthrough, or a new application discovered. That was a challenge: how can businesses and consumers get a grip on emerging tech if the pace of change was so rapid and, in some cases, disruptive?

Internet of Things (IoT) devices are expanding exponentially, and technology breakthroughs reported on the news are almost a daily occurrence. As the adage states, yesterday's science fiction is today's science. We are now expanding our capabilities in every area of science, chemistry, biology, physics, and engineering. That includes heightened space exploration, autonomous cars, as well as building smart cities, new manufacturing hubs, nanotechnologies, 3D printing, and now developing artificial intelligence (AI) and quantum technologies.

And the use of computing, both for performance and security, is being heavily affected in good and bad ways by AI, the IoT, 5G, and quantum technologies with an overriding mesh of cybersecurity.

There is almost too much rapidly morphing information to share, but the topics are too important not to try to tackle and inform.

So my approach to writing this book was to be pragmatic, as it is impossible to "boil the ocean" on the aforementioned subject matter areas that are so expansive and evolving. However, understanding the fundamentals of these technologies, trends, and potential can be communicated. So, I decided to write this book as a primer on how to understand and assimilate impactful technologies on the horizon. To provide useful and thought compelling information on the topics. And specifically, how AI, IoT, 5G, and quantum computing will transform our ways of business, communications, privacy, and especially our security.

Unfortunately, all of us are now at risk of cyberattacks in both our work and personal lives. Most of us, especially the younger generation, live on our smartphones. Everything we do and say on social media can become digitally permanent. When we drive our cars, we no longer rely on paper maps but on our GPS. Soon they also may become autonomous. Our lights, heating, ovens, and other IoT devices are connected and integrated into our lifestyles.

And everyone is beginning to realize that AI is going to significantly change our lives for planning, logistics, and predictive

analyses. Add soon-to-be quantum technologies to the mix, and the future has indeed arrived. But are we prepared?

Although we may welcome this new world of emerging technologies, understanding the risks and how to help reduce them is the biggest challenge we may face. Every sector and technological connection now needs to be safeguarded.

So, with those realities and experiences in mind, I sought to write a book that could provide guiding information and frameworks for the layperson, scholar, and professional alike. Understanding what is inside of cyberspace is therefore a central theme throughout and that is where it begins.

Starting with the digital ecosystem overview, I break down the chapters sequentially by their thematic technology applications. I set the theme of cybersecurity in the first part of the book, then follow up on the key emerging technologies affecting us throughout the following chapters, and culminate it in a discussion of strategies, solutions, and what the future may bring, but under the backdrop of cybersecurity as the digital glue that brings them all together securely.

I have only touched on a few of Industry 4.0s potential consequences and the societal effects of our new technology era. The good news is that our comprehension of technology and its uses is expanding at an exponential rate as well. However, benefits come with risks; thus, society's actual need is preparation and adaptability. Otherwise, we risk losing control of the potential that technological progress has.

My summaries and descriptions serve only as a springboard for learning about how developing technologies will affect our way of life today and beyond. I hope you'll do more research to dive deeper in the areas and technologies that interest you most.

Let me start that quest for you by setting the table with an overview of the technologies and what constitutes the cybersecurity risks and requirements to adapt to this newly merged physical and digital world.

CHAPTER 1

An Overview of Our Merged Physical and Digital Worlds and Cybersecurity

We are now living in a disruptive era of technological growth known as the Fourth Industrial Era. The merging of digital, physical, and biological systems is referred to as the Fourth Industrial Revolution (4IR), or Industry 4.0. This new period of development is radically changing economies, societies, and industries.

Klaus Schwab, the founder, and executive chairman of the World Economic Forum (WEF), is credited with coining the phrase *fourth industrial revolution*. This idea was first presented in his 2016 book with that name. In it, he talks about how new technologies that are starting to intersect with the digital, biological, and physical worlds—such as artificial intelligence (AI), the Internet of Things (IoT), and robotics—have transformed entire industries, economies, and communities.[1]

We find ourselves depending more and more on the complex web of linked systems and gadgets that support our contemporary existence as the digital fabric of our lives keeps growing. With this Malthusian growth and exponential development of human and technological connectivity comes risk, especially in the cyber digital realm, which is the symbiotic connection between technologies and digital security. It includes innovation, productivity, privacy, and ethics, but cyber digital is most commonly referred to as the cybersecurity element. The complexity of cybersecurity dangers and their

worldwide repercussions have significantly expanded in the past few years due to a difficult geopolitical environment and changing technologies.

Emerging technologies are having a wide range of effects on cybersecurity strategies. The overall value of digital transformation for industry and society might reach over $100 trillion by 2025, according to a recent announcement made at the annual WEF gathering in DAVOS.

The announcement touched on the amazing potential:[2]

> Examples of societal value generated by digitization include mass adoption of autonomous vehicles and usage-based car insurance, which could save up to 1 million lives a year worldwide by 2025. In the electricity sector, a cumulative reduction in carbon emissions worth $867 billion by 2025 could be achieved through the adoption of digital technologies, principally through smarter asset planning.
>
> The pace of innovation can be illustrated by the fact that, while it used to take Fortune 500 companies an average of 20 years to reach a billion-dollar valuation, digital start-ups are reaching the same milestone in just four years. The research suggests that, once limitations preventing the mass-market commercialization of enabling technologies such as battery storage and wireless charging are overcome, the pace of change could accelerate.
>
> However, the digital transformation of industries comes with risks attached that will require careful management by all stakeholder groups. One such risk is inequality, which could be exacerbated if access to digital skills is not made available to all. Another is trust, which has been eroded by growing concerns over data privacy and security. This will only be overcome with improved norms of ethical behaviour.

As the WEF noted, digital technology and cloud-based platforms are fully being integrated into this emerging ecosystem. It will catalyze a new era of innovation and automation that affects many industries and verticals, including finance, energy, security, communications, and health. This is already happening at a rapid pace as businesses

are using public, private, and hybrid clouds and computing is moving closer to the computing edge.

There is little doubt that the COVID pandemic ushered in a new era of exponentially increased digital connectedness, which has altered the security paradigm. Due to the widespread adoption of remote work by many businesses and organizations, as well as the increased interconnectedness of PCs and smart gadgets that are being brought online from all over the world, the digital attack surface has significantly increased. Targets are everywhere for hackers.

The hackers are quite capable and well funded. Most ominous is that various criminal enterprises, belligerent nation-states, and loosely associated hackers are among the increasingly sophisticated cyber threat actors. All companies, regardless of size, are now targets that can be reached, and any breach might jeopardize their operations, reputation, brand, and income streams. This also applies to consumers.

By 2025, the research firm Cybersecurity Ventures estimates that the cost of cybercrime will amount to $10.5 trillion from multi-vector breaches.[3] That is a frightening statistic because it is bigger than the gross national products (GNPs) of most economies of countries on the globe.

Five Reasons for the Increase in Cyberattacks

The increasing frequency and potency of cyberattacks is not surprising. The number of cyber breaches is still rising for several reasons. In this section I share just five of them, but they are key ones to consider.

For one thing, as more people and data go online globally, the surface area for cyberattacks grows. This implies that there will be more chances for malware to infect computers and for targets to become digital. The increasing number of computers and devices people connect to means more opportunities for phishing and distributing malware.

Hackers who are motivated by financial gain tend to target the low-hanging fruit. Working from outside the office has changed the paradigm of cybersecurity by expanding the attack surface area. That led to essentially millions of connected offices. The quick shift to remote work brought about by COVID-19 made businesses'

already inadequate cybersecurity readiness profile even worse. The increased attack surface situation increased the temptation for cybercriminals to exploit weak home office and remote work device defenses through ransomware, spear phishing, credential stuffing, and other illegal methods.

Although the COVID scare has diminished, it is estimated that nearly half the US labor force is still working from home. Home offices are not as protected as the fortified office sites that have more secure firewalls, routers, and access management run by their security teams. So, if you are one of those people working remotely, make sure you have upgraded security on your devices and certainly a backup of your critical data!

Second, the sophistication and skill of cybercriminals have increased, as shown in their cyberattacks. Hacker tools are readily available everywhere, and in addition, cybercriminals are using AI and machine learning tools to automate their attacks. Their attacks are now more deadly, more calculated, and faster as a result. Businesses are no longer protected by obscurity because hackers can now spread malware to anybody and automate vulnerability scans.

The use of ultra-realistic visuals and mimicry has made social engineering and phishing intrusions more accessible. It is more difficult to recognize a phish. The days of receiving misspelled bank emails from princes overseas and being asked to click through to receive money in an account are long gone.

What is even scarier is, according to the Swiss Cyber Institute, 1.5 million new phishing websites are made monthly.[4] It is probably a lot more than that because they have to be detected to be counted.

The basic cyber reality nowadays is that anyone can easily fall for a targeted phish, especially if it pretends to be an email from a higher-ranking employee. CEOs in particular are not immune to clever spear phishes.

Third, hackers and the dark web are more likely to exchange advanced hacking kits and tools. When the bad guys find a vulnerability, they usually spread it quickly throughout their groups. Marketplaces selling "zero-day exploits" have occasionally appeared on the dark web; sadly, it is difficult to shut them down fast enough before significant harm is done. Zero-day exploits are a type of cyberattack that use a security hole in software, hardware, or code

that hasn't been fixed yet. This is compounded because many businesses continue to use antivirus software that is outdated and is not patched, even despite efforts to promote cyber hygiene.

Fourth, the emergence of cryptocurrency has made it simpler for criminals to get paid for ransomware. Hackers like to use cryptocurrencies or prepaid bank cards because they are difficult to trace.

And crypto can be a target in itself for hackers. The fact that cryptocurrencies like Bitcoin and others are kept in digital wallets rather than banks has made them targets for hackers. Because these wallets lack the levels or layers of cybersecurity protections required to safeguard the currency owners, they are an ecosystem of easy targets. Hackers can use covert software to mine cryptocurrency on your computer in addition to ransomware.

Fifth, the extreme paucity of qualified cybersecurity professionals in the field has created vulnerabilities and opportunities for criminal hackers. There are not enough skilled cybersecurity workers to handle demand and counterattacks. Both the public and private sectors find it challenging to stay up-to-date with the most recent malware patches and to continuously monitor the ever-evolving threat horizon as the volume and cost of breaches continue to rise. Unfortunately, there does not seem to be light at the end of the tunnel in solving the global shortage of cyber technicians despite many efforts to attract people to the field.

Knowing how to write algorithms and code is undoubtedly part of most cybersecurity career paths, but it goes well beyond that. In addition, it includes aspects of discipline such as thought leadership, policymaking, senior management, compliance, marketing research, intelligence, and technology foraging. Both a will to learn and possessing soft skills are necessary for success in this area. More people need to be encouraged to pursue cybersecurity career pathways.

To increase the number of cybersecurity workers, more must be done to draw women into the field and to retrain veterans to fill skills gaps. My thought is that it would also be wise for government, academia, and industry to put in a great deal of effort to train and invest in Native Americans, who have a long history of supporting national security in government, to develop the next generation of cybersecurity technicians and data analysts from a variety of urban and rural

economically disadvantaged areas. I have proposed that in several articles I have written.

Cyber Wake-Up Calls, Breaches, and the Need to Catch Up

We also need a new approach in building cyber defenses with emerging threats. Both business and government cybersecurity efforts have focused on responding to the most current security flaws or threats in recent years. This is a reactive rather than proactive approach, and consequently cyber defenders were always at least one step behind, making it challenging to mitigate the risks.

Many wake-up calls, such as a significant string of sophisticated threat actor intrusions against numerous high-profile targets (such as SolarWinds, Colonial Pipeline, OPM, Anthem, Yahoo!, and many more), have exposed a defective strategy for data defense and operating with a passive preparedness, which has led to a shift in the reactive mindset.

As a consequence of the sharp rise in security breaches and the increased awareness of how crucial IT is to our operations, safeguarding against breaches is now seen as more than just an expense for the company; rather, it is essential to maintaining reputation and business continuity. Both businesses and governments have been taking a more proactive approach to cybersecurity to fix the broken model.

Despite the increasing frequency, sophistication, lethality, and liabilities linked to intrusions, industry management has largely lacked readiness and moved slowly to strengthen cybersecurity. Businesses are facing more and more cyberattacks; therefore, the C-suite needs to act quickly and prioritize asset protection, especially sensitive data. And they need to invest more in both people and resources.

It is a time of transition for many organizations and provides opportunities to fill gaps and change security postures. To consolidate and safeguard data, a lot of businesses and organizations are moving their data from legacy systems to cloud, hybrid cloud, and edge platforms.

We are also experiencing cyber flux. New operational shifts brought about by emerging technologies like 5G, the IoT, AI, and

quantum technologies will necessitate new cybersecurity risk management approaches. A major problem is adaptability and scalability to upgrade to new security technologies and processes, given the broad variety of architectures, systems, and jurisdictions. Certainly, this is the right moment for businesses to be proactive in cybersecurity.

In summary, for all the reasons this chapter discussed about growing connectivity and adversarial sophistication of attacks, ultimately, whether you are a corporation or an individual, your cybersecurity posture must adopt a preparedness-based mentality instead of a passive one. Any business, regardless of size, is now a target in the modern digital environment. A breach might jeopardize a company's operations, reputation, brand, and income streams. Or you might be put out of business by just one breach.

Admittedly, it can be difficult to stay on top of cybersecurity concerns because of the rapid pace of digitization and change. This challenge is particularly difficult with the evolving cyber threats and digital convergence, the topic of Chapter 2.

CHAPTER 2

Cyber Threats, Targets, and Digital Convergence

To understand where we are digitally today, it is important to know how it started and get to the roots of the security problems. It started from the digital inception. The internet was created in a government laboratory by the Department of Defense's DARPA (the Defense Advanced Research Project Agency), and corporate vision was responsible for institutionalizing and commercializing it, ushering in a new era of technological and social revolution.

However, it was created to facilitate communications, and security was not given top priority. As a result, it developed more quickly than security procedures and did not adopt preventative measures. Hence it became the Wild West of interconnectivity and risk.

The Root of the Security Problem Explained

Joel Brenner, a former counsel to the National Security Agency sums up the current state of cybersecurity:

> The Internet was not built for security, yet we have made it the backbone of virtually all private-sector and government operations, as well as communications. Pervasive connectivity has brought dramatic gains in productivity and pleasure but has created equally dramatic vulnerabilities. Huge heists of personal information are common, and cyber-theft of

intellectual property and infrastructure penetrations continue at a frightening pace.[1]

The security problem that was apparent from its inception has been exacerbated by an evolving digital ecosystem of convergence and interdependency. Our everyday financial activity, credit cards, and bank accounts are all linked. Even our interpersonal communications via smartphones at social media applications have become a playground for cyberattackers. All of our records—including private medical histories—are shared digitally and managed by algorithms.

These days, we live in an immersive algorithmic environment. Algorithms are generally defined as a mathematical procedure for solving a problem in a finite number of steps. In the context of the developing digital world, each computer program must have algorithms because they are the foundation of many different applications and systems, including search engines and navigation systems. The algorithms are unleashed and multiplying.

Cyber Safety: The Nature of the Problem

It is understandable why there is a digital predicament. The growing interconnectedness and digital commerce across industries have had major ramifications for privacy and security, especially due to vulnerabilities in digital logistics and secure communications. Everything connected online, whether it is devices or people, can be a target of a malicious digital intruder.

At the highest levels, organizations, both large and small, are awakening to the fact that cybersecurity can no longer be ignored or deferred to the IT department or quarterly board meetings. They do so at their peril.

The scarier part is that the digital ecosystem is becoming more precarious day by day. Viruses, ransomware, and other malicious software that affect our digital interface are appearing more frequently because it has become so easy to spread by criminal hackers. The most popular and easy forms of cyberattacks are social engineering, ransomware, insider threats, distributed denial of service (DDOS) attacks, and spear phishing, particularly targeted at