BITSKRIEG

THE NEW CHALLENGE OF CYBERWARFARE

JOHN ARQUILLA

Table of Contents

Bitskrieg

The New Challenge of Cyberwarfare

John Arquilla

polity

Copyright Page

First published in 2021 by Polity Press

Polity Press

65 Bridge Street

Cambridge CB2 1UR, UK

Polity Press

101 Station Landing

Suite 300

Medford, MA 02155, USA

ISBN-13: 978-1-5095-4362-5

ISBN-13: 978-1-5095-4363-2 (pb)

A catalogue record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication Data

Names: Arquilla, John, author.

Title: Bitskrieg : the new challenge of cyberwarfare / John Arquilla.

Other titles: New challenge of cyberwarfare

Description: Cambridge ; Medford : Polity Press, 2021. | Includes bibliographical references and index. | Summary: “Pioneer of the concept of “netwar” explains why Bitskrieg is here to stay”-- Provided by publisher.

Identifiers: LCCN 2020057162 (print) | LCCN 2020057163 (ebook) | ISBN 9781509543625 (hardback) | ISBN 9781509543632 (paperback) | ISBN 9781509543649 (epub)

Subjects: LCSH: Cyberspace operations (Military science) | Information warfare. | Deterrence (Strategy) | Computer security.

Classification: LCC U167.5.C92 A77 2021 (print) | LCC U167.5.C92 (ebook) | DDC 355.4/1--dc23

LC record available at https://lccn.loc.gov/2020057162

LC ebook record available at https://lccn.loc.gov/2020057163

by Fakenham Prepress Solutions, Fakenham, Norfolk NR21 8NL

The publisher has used its best endeavors to ensure that the URLs for external websites referred to in this book are correct and active at the time of going to press. However, the publisher has no responsibility for the websites and can make no guarantee that a site will remain live or that the content is or will remain appropriate.

Every effort has been made to trace all copyright holders, but if any have been overlooked the publisher will be pleased to include any necessary credits in any subsequent reprint or edition.

For further information on Polity, visit our website: politybooks.com

Dedication

For Peter and Dorothy Denning

Epigraph

The modern age has a false sense of superiority because of the great mass of data at its disposal. But the valid criterion of distinction is rather the extent to which man knows how to form and master the material at his command.

Johann Wolfgang von Goethe (1810)

Knowledge must become capability.

Carl von Clausewitz (1830)

[Cyber attacks] can actually bring us to our knees.

Admiral Mike Mullen (2011)

There are only two types of companies: Those that have been hacked and those that will be.

Robert Mueller (2012)

Acknowledgments

It has been my privilege, over the past four decades, to sit beside and learn from some of the finest minds, and individuals, dedicated to understanding the implications of the Information Age for society and security. Early on, at RAND, Willis Ware made me aware that, for all the good connectivity brings, vulnerability is its inevitable flip side. Tom Rona understood that cyberwar was going to have profound effects, one day, on battle. Captain Richard O'Neill, USN (Ret.) knew this, too, and convinced higher-ups in the Pentagon that the work my research partner David Ronfeldt and I were doing merited their support. Dick also helped found our Highlands Forum, which had a 20-year run raising awareness about Cyber-Age issues that matter. Technology journalist John Markoff and futurist Paul Saffo are both responsible for expanding my mind. As are some of the world's top hackers, especially "M" and "MHN." At the Naval Postgraduate School, Peter and Dorothy Denning, to whom this book is dedicated, have shared their insights and helped me to sharpen my thinking. As has Ryan Maness. For many years, the Honorable Leon Panetta and his wife Sylvia have welcomed me into the cyber activities of the Institute they oversee. At Polity, Louise Knight is all one could ever ask for in an editor: affirming, wise, assertive when needed.

Foreword

Communication and information lie at the heart of victory in war. The ability to communicate securely and ascertain the movements of the enemy correctly are the foundation of the safety of troops and the confidence of leadership. With the need to communicate over vaster and vaster distances, however, came hidden risks – the adversary could more easily access that information. Well-known examples are those of the Allied advantage in World War II with the successful breaking of both the German and Japanese coded battle information – the Ultra and the Magic intercepts.

Today, we have entered an even more dangerous era, an era that will call upon our entire nation's resources – material, to be sure, but moral and intellectual as well. Very small numbers of persons utilizing modern computers can deal devastating losses to advancing armies and to civilian populations. Some experts in cyberwarfare have conjectured that there may never be a final victory in cyberwars. Rather, victory may well involve merely avoiding defeat.

In the history of warfare, the initial periods when new weapons were developed were often the most dangerous. The possessors of the new technology saw themselves as having a unique advantage, but one that was fleeting, creating a "use it or lose it" mentality. It was also the period when the technology and its consequences were least understood. The result was devastation unequaled for the time.

John Arquilla's *Bitskrieg: The New Challenge of Cyberwarfare*, an eloquent and lucid study, peppered with relevant historical examples worthy of a book themselves, provides a valuable analysis that will inform both a general audience and the cyber expert. Arquilla argues that: “Cyberwar would entail changes in each of these areas: e.g., from larger formations to smaller, nimbler, highly networked units; from mass-on-mass engagements to supple swarm battle tactics; and to the larger strategic goal of ‘knowing more’ than the enemy – about the composition, disposition, and intentions of the forces on both sides.” He brings the reader up to date on the latest advances in cyberwar – against an enemy that is anonymous, projecting force disproportionate to its size, strength, or wealth.

Arquilla acknowledges that the United States projects a confirmed military superiority in its aircraft carriers and the planes that they carry, as well as a nuclear arsenal of the highest quality. But the easy access of information power on the Internet changes this advantage. A country like Iran with gunboat swarming tactics, or North Korea with cyberwarfare, can neutralize this seemingly invincible force. In the cyber domain, even small non-state actors can challenge the superpowers.

These challenges were known and feared when I served as Director of the CIA and Secretary of Defense (2009–13). Seven years, however, in the cyber era is more like a century of change in former times. So, in a manner of speaking, Arquilla picks up where my responsibilities left off. He focuses on the latest developments in cyberwarfare and the need for: secure connectivity and information; a major change in the US military and its organizational design and configuration; and a commitment to arms control negotiations related to cyber.

Regarding the security of connectivity and information, he makes a strong case for encryption and utilization of Cloud computing. In the area of military and security affairs, he argues convincingly about swarm tactics (small networked teams on the ground, connected with each other and attack aircraft) successfully engaging a larger enemy. He also emphasizes the necessity to move from a hierarchical to a networked perspective regarding information flows and organizational forms that were tailored for the industrial age, but are no longer effective today. Finally, he argues convincingly for international meetings that take seriously the idea of cyber arms control.

Indeed, Arquilla argued for cyber arms control negotiations as early as the 1990s, to no avail. At the time, the United States led the world in cyber and it was presumed that that edge would last. While the United States still has the edge offensively in the world of cyber, the Russians and the Chinese lead defensively. In fact, Arquilla argues that Iran’s and North Korea’s defensive capabilities in cyber are more advanced than those of the United States. And he discusses the reasons why open societies have been at a disadvantage in developing secure cyber defenses.

These are only a few of the ideas and revelations presented in this fast-paced, lively study. There is much, much more that will add depth and breadth to the reader’s understanding of the cyber challenges that face the United States and the world. As Secretary of Defense, I warned that the United States was vulnerable to a cyber “Pearl Harbor.” The threat of a cyber attack that shuts down our electric grid, and financial, government, chemical, transportation, and other infrastructure systems, is real. Arquilla’s handling of this complex subject is deft and clear-eyed. His love of the United States, and his work toward keeping us safe and secure, place him among the leading national security thinkers of our time. He is presenting a wake-up call to the nation that will determine whether we are prepared to deal with the cyber threats to the security and safety of our democracy.

Leon E. Panetta

Preface

In the wake of the devastating Japanese attack on Pearl Harbor in December 1941, and the rain of hard blows that soon followed, American Secretary of the Navy Frank Knox mused publicly that “modern warfare is an intricate business about which no one knows everything and few know very much.” Yet, within just six months, the tide turned against Japan at the Battle of Midway; and by the end of 1942 the Germans were decisively defeated in grinding land battles at El Alamein and Stalingrad. The Allies quickly learned to use aircraft carriers as the “tip of the spear” in sea fights, and that tank–plane coordination was the key to *Blitzkrieg*-style armored breakthroughs in land battles. Diffusion of the best warfighting practices happened quickly during World War II, and the methods developed in that great conflict have continued to shape much of military strategy in the more than 75 years since its end.

But swift adaptation has hardly been the case in our time, an era of emerging “postmodern” warfare. For decades, the dark, predatory pioneers of cyberwar have proved consistently able to overcome defenses and enjoy sustained freedom of action. In terms of cyberspace-based political warfare, for example, the Russians have proved masters, hitting at electoral processes in the United States and across a range of other liberal societies. Faith in the accuracy of the voting processes so vital to democracy has been undermined. China, for its part, has developed a high degree of skill at accessing and absconding with the cutting-edge intellectual property of a range of firms around the world. Mid-level powers such as North Korea have also shown considerable muscle in what might be called “strategic criminal” aspects of cyberwar, the proceeds of such larceny used to support their governments’ nefarious activities, not least in the realm of nuclear weapons proliferation.

Even non-state actors of the more malevolent sort, from terrorists and militants to hacker cliques, have used cyberspace as a kind of virtual haven from which to operate. All have, one way or another, learned how to “ride the rails” of advanced technological systems, exploiting their vulnerabilities and using them as launching points for infrastructure attacks, theft of money, and more. Emergence of the Internet of Things (IoT) has only strengthened these disruptors – both hostile nations and dark networks – as now they can mobilize hundreds of millions of connected household devices to serve in their zombie networks. The current situation, far from seeing an equilibrium arise in which offensive and defensive capabilities are balanced, is one in which attackers retain the advantage because defenders rely overmuch on the least effective means of protection: Maginot-Line-like firewalls and anti-virals that are always a step behind advances in malicious software.

Clearly, one of the principal challenges today is to improve defenses. In my view, this would be by ubiquitous use of strong encryption and regular movement of data around and among the Clouds – that is, others’ data systems. The Fog, consisting of the available portions and lesser-mapped areas of one’s own information space and capacity, can also provide improved security, easing the fundamental problem that “data at rest are data at risk.” But even a very robust remote storage and movement system cannot substitute for strong encryption; weak codes will invite acts of cyber aggression. Unfailingly.

Aside from the way poor cybersecurity leaves societies open to having both their politics and their prosperity undermined, there is another risk: that disruption of Net- and Web-connected military communications will lead to wartime disasters – in the field, at sea, and in the aerospace environment. Future battles between advanced armed forces will be incredibly fast-paced, replete with weapons empowered by artificial intelligence and coordinated to strike in networked "swarms." A military whose reflexes are slowed by the kinds of disruption computer viruses, worms and other cyber weaponry cause will find itself at risk of being outmaneuvered and swiftly defeated. This aspect of cyberwar – focused on "battle" – is the successor to World War II's *Blitzkrieg* doctrine; I call it *Bitskrieg* to draw the analogy with that crucially important previous inflection point in military and security affairs.

The dangers posed by the more familiar aspects of cyberwar, from political disruption to criminal hacking and potential infrastructure attacks, pale next to the consequences of failing to see that military operations can be fatally undermined by information insecurity. That is why the need to start paying serious, effective attention to armed-conflict aspects of cyberwar is urgent. But the scope and variety of cyber threats are daunting, making it difficult to address all, especially given the attention-grabbing nature of the latest incident of one sort or another. This suggests that there is one more important, also unmet, challenge that should be taken up alongside efforts to improve cybersecurity and prepare to wage *Bitskrieg*-style field operations: arms control. Since virtually all advanced information technology is "multi-use" – employable for commerce, provision of services, social interaction *or* war – the nuclear model of counting missiles and controlling fissile material will no longer do. This has led many (well, most) to scoff at the very idea of cyber arms control. But there is another paradigm that is based on behavior, rather than “bean counting.” It has worked well, for many decades, with the Chemical and Biological Weapons Conventions – covering types of deadly arms whose basic materials can be fabricated by countless countries – whose signatories have covenanted never to make or use such devices. A similar, behavior-based approach to cyber arms control is possible as well.

The need to protect individuals, intellectual property, infrastructures and elections from cyber attack is hardly new; the way to meet challenges to them that I advance is. “New” in the sense that the current approach to cybersecurity, so reliant on firewalls and anti-virals, should for the most part be jettisoned in favor of the strongest encryption and the widespread use of Cloud and Fog computing. The failure of existing security systems is so overwhelming, as the reader will see, that the need to shift to a new security paradigm is now well beyond urgent. As a wise American chief of naval operations once said to me about cyber threats, “The red light is flashing.”

And, with armed forces and armed conflict in mind, I argue herein that the direct, warfighting implications of advanced information technologies – including artificial intelligence – have received too little attention for far too long. The fundamental problem is that a wide range of these new tools have simply been folded into or grafted onto older practices. Thus, the shift from *Blitzkrieg* to *Bitskrieg* has not yet been made. My goal is to make sure that aggressors don’t make this leap first. The painful lessons inflicted by the Nazi war machine from 1939 to 1941, at the outset of the Mechanization Age, should sensitize us to the potential cost of failing to parse the profound implications for warfare posed by the Computer Age. A cost that will surely be imposed should cyber challenges to society and security remain unmet.

Aside from illuminating the current challenges that must be met and mastered if peace and prosperity are to have a reasonable chance of thriving as we look ahead, I also “look back” in two principal ways. One aspect of this retrospection focuses on linking current – and future – issues in military affairs and information security systems to what has gone before. The best example of this tie to earlier history is the manner in which, during World War II, the Allies, using the world’s first high-performance computers, “hacked” the Axis and won critical victories in desperate times, often when the odds were stacked heavily in favor of the aggressors, as at the Battle of Midway in June 1942. The knowledge advantage that the Allies possessed over the Axis played a crucial role in the latter’s defeat. Clearly, mastery of the information domain has long mattered; it matters just as much to victory today, and will only grow in importance over the coming decades.

The second way in which I engage in retrospection reflects my own experiences and ideas in this field over the past 30-plus years, in war and peace. As I look back, from early debates about the strategic implications of the Information Age *circa* 1990 to very recent times, I find that, Forrest-Gump-like, I have been present at many high-level American policy debates about the various dimensions of cyberwar, and have sometimes played an active role in events.

The reflective passages, the reader will find, offer a range of first-time revelations about: how the information advantage over Saddam Hussein enabled General Norman Schwarzkopf to opt for the daring “left hook” plan that was the heart of Operation Desert Storm; why the 78-day air campaign during the Kosovo War did so little damage to Serbian forces; what went on at the first Russo-American meeting of cyber experts; and where the current debates about the military uses of artificial intelligence are, and where they are headed. It has been a privilege to be involved in these and a range of other cyber-related events over the years. But having a privilege is hardly the same as witnessing real progress, and of the latter I have seen far too little. Perhaps this book will stimulate a renewed, and broader, discourse about cyberwar before the Age of *Bitskrieg* opens with a thunderclap upon us. I hope so.

John Arquilla
Monterey, December 2020

1
"Cool War" Rising

The German philosopher of war, Carl von Clausewitz, described armed conflict as "a true chameleon" whose three base elements are "primordial violence . . . the play of chance," and, ultimately, its "subordination as an instrument of policy."[1] He had no way of knowing, some two centuries ago, how prescient his notion of the chameleon-like character of warfare would prove to be in its Information-Age incarnation. Echoing Clausewitz, strategist Martin Libicki has described cyber conflict as a "mosaic of forms" ranging across the various modes of military operations, and having significant psychological, social, political, and economic aspects as well. As to Clausewitz's element of primordial violence, Libicki has contended that cyberwarfare slips the bonds of traditional thinking about armed conflict. Of its many manifestations, he has argued, "None of this requires mass, just guile."[2] This poses some very major challenges to those who would defend against cyber attacks, given that the lack of requirement for mass means that small nations, networks of hackers, even super-empowered smart individuals unmoored from any Clausewitzian notion of a guiding policy, can wage a variety of forms of warfare – operating from virtually anywhere, striking at virtually any targets.

Cyber attackers, whoever and wherever they are, can opt to disrupt the information systems upon which armed forces' operations increasingly depend – on land, at sea, in the air, even in orbit – or take aim at the control systems that run power, water, and other infrastructures in countries around the world. This mode of attack can also foster crime, enabling the theft of valuable data – including cutting-edge intellectual property – from commercial enterprises, the locking-up of information systems whose restoration can then be held for ransom, or simply the exploitation or sale of stolen identities. The democratic discourse can easily be targeted as well, allowing a whole new incarnation of political warfare to emerge in place of classical propaganda – as demonstrated in the 2016 presidential election in the United States,[3] but which can be employed to disrupt free societies anywhere in the world. And for those attackers of a more purely nihilistic bent, controlled or stolen identities can be conscripted into huge "zombie" armies deployed to mount distributed denial-of-service (DDoS) attacks aimed at overwhelming the basic ability to operate of the targeted systems – institutional, commercial, or individual. When billions of household appliances, smartphones, and embedded systems (including implanted locator chips in pets) that constitute the Internet of Things (IoT) are added as potential "recruits" for cyber attackers' robot networks ("botnets"), the offensive potential of cyberwarfare seems close to limitless.

And all this takes, as Libicki has sagely observed, is *guile*. Thus, it seems that, aside from providing a strong affirmation of Clausewitz's general point about conflict having chameleon-like properties, the many faces of cyberwar undermine his three base elements. There is no need to commit acts of overarching violence, or even for a connection to higher-level policy, when, for example, millions of "smart refrigerators," designed to send their owners an email when they need milk, can be hacked, controlled, and ordered to overwhelm their targets with millions of emails. As to chance, the vast range of targets available to cyber attackers – who often remain hidden behind a veil of anonymity, a "virtual sanctuary" – suggests that luck is a much less included factor. This undermining of Clausewitz’s base elements leads to a serious challenge to his firmly held belief that “defense is a stronger form of fighting than attack.”[4] This was certainly the case in his time, when defense-in-depth defeated Napoleon in Russia, and later saw the Duke of Wellington’s “thin red line” decimate the *Grande Armée* at Waterloo. A century later, the costly failed offensives on the Western Front in World War I affirmed the wisdom of Clausewitz. And even the brief period of *Blitzkrieg*’s success in World War II gave way, from El Alamein to Stalingrad to the Battle of the Bulge, before stout defenses. But, two centuries since Clausewitz, the rise of cyberwar is now upending his unwavering belief in defense dominance. Instead, offense rules.

To date, the best-known manifestations of cyberwar have emerged in the personal and commercial realms. Hundreds of millions of people around the world have had their privacy compromised, either by direct hacks or by having their information stolen from insurance, financial, retail, social media, and government databases. With regard to ostensibly “secure” government databases, even these have proved porous. The most notorious incident was acknowledged by the US Office of Personnel Management in June 2015. Of this intrusion, in which hackers accessed sensitive personal information, the President of the American Federation of Government Employees, James Cox, asserted “all 2.1 million current federal employees and an additional 2 million federal retirees and former employees” were affected.[5] (My own classified personnel file was among those hacked.) As the matter was investigated further, the estimated number of persons affected quintupled, to more than 20 million, according to Congressional testimony of the then-Director of the Federal Bureau of Investigation, James Comey, given just a month later.[6] But even this staggering breach paled in comparison with the revelation in May 2019 that *nearly 900 million* sensitive financial records had been hacked from the database of the First American Title Company.[7]

As to the theft of intellectual property and other types of exploitative or disruptive cyber attacks aimed at commercial enterprises, these cause more than 1 trillion dollars ($US) in damages each year. University research centers are also targeted as, according to one tactful report, they “haven’t historically been as attentive to security as they should be.”[8] While the ransoming of locked-up information currently accounts for less than 1% of annual losses, this mode of attack is growing at a steep rate.[9] Often, such theft and extortion aim at serving causes beyond just enrichment of the malefactors. In the case of North Korea’s cyber crimes, the United Nations has reported that the roughly $2 billion gained as of mid-2019, by attacks on banks and crypto-currency (e.g., Bitcoin, Ethereum, Ripple) exchanges, has been used to support its nuclear weapons program.[10] This illicit form of fundraising lies somewhere between theft and statecraft. Call it “strategic crime.” Much as, in the sixteenth century, Queen Elizabeth I tacitly encouraged her piratical “sea dogs” to prey upon maritime commerce to help fill Britain’s coffers. Strategic crime has long played a role in statecraft via this form of naval irregular warfare.[11]

Clearly, when it comes to the abovementioned modes of cyber attack, offense is currently quite dominant. And, as George Quester’s seminal study of stability and instability of the international system notes, when the apparent risks and costs of taking the offensive are low, conflicts of all sorts are more likely to proliferate.[12] They may be small-scale, individually, but their cumulative effects are large – and growing – as opposed to the more purely military realm, in which the patterns of development and diffusion are less apparent. So much so that, to some analysts, the emergence of militarized cyberwar seems highly unlikely.[13]

Cyber attacks in armed conflicts *have* had a lower profile, but there are some troubling examples – most provided by Russia. In 2008, when Russian troops and Ossetian irregulars invaded Georgia, the defenders' information systems and links to higher commands were compromised by cyber attacks on their communications. Panic-inducing mass messaging aimed at people's phones and computers in areas where the Russians were advancing put large, disruptive refugee flows onto the roads, clogging them when Georgian military units were trying to move into blocking positions. All this helped Russia to win a lop-sided victory *in five days*.[14]

More recently, two other aspects of cyberwar have come to the fore in the conflict in Ukraine between government forces and separatists in Donetsk, with the latter supported not only by Russian irregulars – "little green men," so named for the lack of identifying patches on their uniforms – but also by bits and bytes at the tactical and strategic levels. In the field, Ukrainian artillery units were for some time victimized by hacks into their soldiers' cellphone apps that were being used to speed up the process of calling in supporting fire. Russian-friendly hackers helped to geo-locate artillery batteries by this means, and brought down counter-battery fire upon them. The result: diminution of Ukrainian artillery effectiveness, although the precise extent of losses incurred remains a matter of some debate.[15]

At a more strategic level, the Russo-Ukrainian conflict has also featured a number of troubling attacks. The first came on Ukraine's electrical power grid infrastructure in December 2015, when 30 substations in the Ivano-Frankivsk *oblast* were shut down as hackers took over their