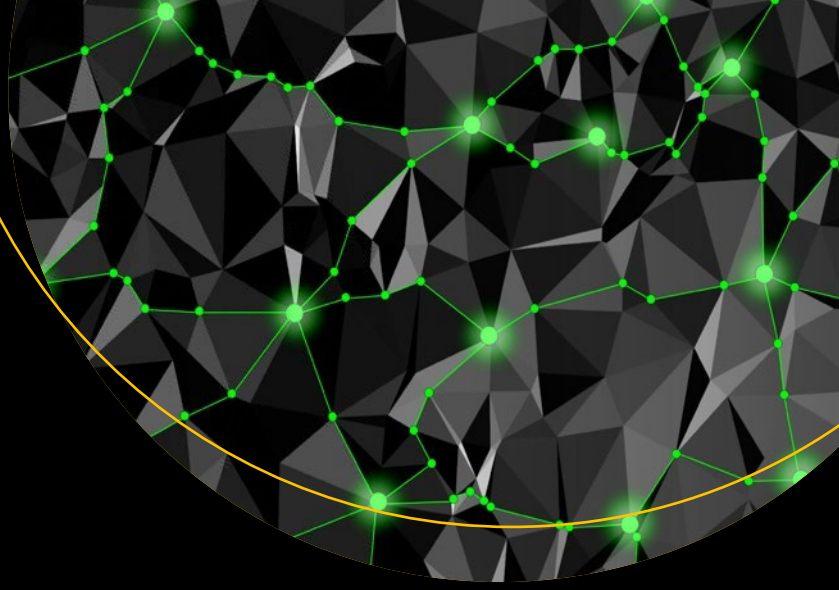

Waging Cyber War

Technical Challenges and Operational Constraints

Jacob G. Oakley

Apress®

Waging Cyber War

Technical Challenges and Operational Constraints

Jacob G. Oakley

Apress®

Waging Cyber War: Technical Challenges and Operational Constraints

Jacob G. Oakley
Owens Cross Roads, AL, USA

ISBN-13 (pbk): 978-1-4842-4949-9 ISBN-13 (electronic): 978-1-4842-4950-5
https://doi.org/10.1007/978-1-4842-4950-5

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484249499. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

To my children, you'll move mountains.

Table of Contents

About the Author

Dr. Jacob G. Oakley spent over 7 years in the US Marines and was one of the founding members of the operational arm of Marine Corps Forces Cyberspace Command, leaving that unit as the senior Marine Corps operator and a technical lead. After his enlistment, he wrote and taught an advanced computer operations course, eventually returning back to mission support. He later left government contracting to do threat emulation and red teaming at a private company for commercial clients, serving as principal penetration tester and director of penetration testing and cyber operations. He is working as a cyber SME for a government customer. He completed his doctorate in IT at Towson University researching and developing offensive cyber security methods. He is the author of the book *Professional Red Teaming* (Apress, 2019) and the technical reviewer of the book *Cyber Operations, Second Edition* (Apress, 2019), by Mike O'Leary.

About the Technical Reviewer

Wayne York is a retired Marine with over 20 years of service and experience ranging from systems administration, digital network analysis, signals intelligence, and cyber operations. He was involved in the stand-up of the Marine Corps Forces Cyberspace Command with nearly a decade spent between the headquarters and operational components. His time in the Marines as a warfighter and cyber operations subject matter expert provides insight into the complexities of the cyberspace domain.

He is now a senior penetration tester with a professional services company and works both commercial and government contracts helping ensure customers secure their networks and applications from adversarial cyber threats. He holds a Bachelor of Science in Computer Networks and Cybersecurity from the University of Maryland University College, as well as Security and Certified Ethical Hacker (CEH) certifications.

Acknowledgments

I thank my beautiful wife and family for sacrificing their nights and weekends to let me write this book and for loving and supporting me through this and other nerdy endeavors.

I thank my father for exemplifying hard work and for all he did to give me the best chance to succeed in life.

I would like to thank Wayne York for being the technical reviewer for this book and being a true leader of Marines, specifically this Marine.

To all you keyboard-wielding cyber warriors out there protecting freedom, I salute you.

Introduction

This book was written to inform the reader on the increasingly intertwined concepts of war and cyber. It is meant to dispel the misconceptions and mythos surrounding cyber warfare. Reading this book will provide insight into the technical obstacles within the cyber domain which hinder effective warfighting operations. You will also come to understand how legal and oversight authorities, as well as international convention, further constrain what technical capabilities do exist. Cyber warfare has crept into facets of everyday life. Each individual citizen and their personal devices, from cell phone to smart fridge, represent an extension of a nation's attack surface. Whether you are a policy maker, commander, warfighter, technical or non-technical citizen, or employed in the cyber security industry, understanding the facts of cyber warfare is necessary to combat its increasing pervasiveness.

CHAPTER 1

Cyber and Warfare

There is an awful lot of hype and confusion surrounding the concept of cyber warfare. It is certainly a term that has gained traction recently in the media and in military and government discussions. As ambiguous as the term cyber is itself, cyber warfare seems to suffer from even more variance and mischaracterization in its definition, doctrine, and implementation. Fortunately, I believe that in understanding warfare and cyber separately we can societally come to a more standardized and widespread acceptance of what it means to defend ourselves in a cyber war, conduct cyber warfare, and perhaps globally define what is and is not acceptable in such conflicts.

To properly understand what it will mean to go to war through cyber means we must unilaterally understand and cede to the truth and challenges that would exist in such combat. We cannot continue to apply known paradigms to a novel concept. "The Charge of the Light Brigade" is regaling and heroic; however, it was decimating and futile, and casualties were excessive. If we keep trying to think of cyber warfare as simply shooting like-sized cyber bullets at our enemy for similar or more improved effect or applying monolithic military doctrine without a technical understanding to cyber warfare, we will fail. Educating people, policy makers, and warfighters has to start somewhere, and I hope that in providing the ground truth of the technical and tactical challenges to waging a cyber war, we can together approach the future of warfare more informed.

Definition

First and foremost, what must be accepted is that war has not changed with the advent of the cyber buzzword. Cyber is just another way to carry out war, just like trench warfare, nuclear warfare, and any of the other categories of warfighting established throughout history. The United States Department of Defense (DoD) established its Cyber Command on October 31, 2010. From its homepage you can read its mission which is "to direct, synchronize, and coordinate cyberspace planning and operations to

J. G. Oakley, *Waging Cyber War*, https://doi.org/10.1007/978-1-4842-4950-5_1

defend and advance national interests in collaboration with domestic and international partners."[1] Now, that does not sound particularly like warfighting, but on August 27, 2017, President Donald Trump decided to elevate USCYBERCOM from a sub-unified command to a Unified Combatant Command responsible for cyberspace operations. Also, from the USCYBERCOM web site, "The decision to elevate USCYBERCOM was seen as recognition of the growing centrality of cyberspace to U.S. national security and an acknowledgment of the changing nature of warfare."

These statements and declarations need some further clarification to really understand where we are going with these concepts. First starters, what is cyberspace? Merriam-Webster defines it as "the online world of computer networks and especially the Internet." The DoD recognized cyberspace as a warfighting domain, which means it is considered to be as encompassing as air, land, sea, or space, which are the other warfighting domains. This means that computer networks are to be viewed as the space within which we can maneuver, attack, and defend just like we do in warfare conducted in the other domains. Merriam-Webster defines war primarily as "a state of usually open and declared armed hostile conflict between states or nations" and warfare as "military operations between enemies." So, a deductive definition of cyber warfare is military operations carried out over computer networks in a declared conflict between state or nation enemies. This may seem like an oversimplification; however, it is the foundation for understanding the challenges of carrying out such military operations.

Declaration

With the workings of a definition for cyber warfare established, we next need to focus on the action that officially initiates war in general, cyber or otherwise, which is a declaration of war. This is an important topic to cyber-specific warfare for many reasons. Regardless of the domain a war is fought in if war is declared by a state; there are ethical, legal, and other implications that now apply to all following actions.

A state goes to war by declaring war in response to an act of war. That is essentially how an acknowledged armed conflict between states would begin. This is quintessentially illustrated by the bombing of Pearl Harbor by the Japanese during World War II. There was an act of war by the Japanese in using uniformed military actors to perpetrate a state-acknowledged act of aggression on US uniformed military actors

[1] www.cybercom.mil/About/Mission-and-Vision/

against targets in US sovereign waters and airspace and on US soil. In response to this, the US Congress, as the body with authority to do so, declared war against the Empire of Japan. The power to declare war is given to the US Congress in article one section eight of the US constitution. For perspective, the United States has only declared war 11 times, beginning with Great Britain in the war of 1812 and last with 6 individual declarations against specific countries during World War II.

It is an interesting thought experiment to ponder what type of cyber act it would take to convince the United States to declare war. Unlike conventional war, an act of war that was solely within the realm of the cyber domain is difficult to conceive. Slightly more analogous might be a cyber-enabled effect, where the cyber domain is used to control or effect some physical asset that might have widespread mortal effects worthy of a declaration war. Even this is extremely challenging as adequately attributing such an action to a state without an admission from that state is nearly impossible, we will cover more on that later. At this point we can essentially make two summations regarding cyber and warfare.

First, a cyber act of war almost assuredly will involve a cyber-physical connection and not simply stay within the realm of cyber. For instance, an attack fully within the cyber domain using a virus which cripples computers across all air force air bases is highly impactful to our national defense, but not likely to draw the US Congress into declaring war against the perpetrator. On the other hand, an attack that uses a computer virus to simultaneously take over the computers on nearly 100 air force aircraft involved in a large annual exercise and crash them all into the desert, killing nearly 1000 uniformed soldiers might be enough to result in a declaration of war against the perpetrator.

Second, with the exceedingly difficult obstacles to reliable attribution of cyber actions, the perpetrator of a cyber act of war would almost have to do so with the intent of acknowledging that action and starting a war. Even in the huge aggression of the cyber-physical example where billions of dollars in damages, thousands of deaths happen in a US sovereign area, if no perpetrator admits to the attack, what requirements must there be on an attribution to convince Congress to declare war on what they think to be the perpetrator. We will cover attribution in several chapters later in this book, but even at this juncture, trying to discern the type of proof Congress would require to declare war seems a daunting, if not impossible, task.

Even with the establishment of cyber warfare, it is only one of many warfighting domains, and Congress would have to be comfortable enough in the impact and

identification involved in a cyber act of war to respond with armed conflict in all warfighting domains. As entertaining as the idea may be, I don't think the United States is going to respond to malicious email solicitation by a Nigerian Prince by sending aircraft and naval vessels and deploying troops to Nigeria after performing intercontinental missile strikes on their military bases. The ridiculousness of this example is easy to see, coming up with what credible cyber act deserves such a response is nowhere near trivial.

Just War Theory

Just war theory is essentially a set of requirements that must be met for a war to be considered just. It focuses on two essential criteria, the right to go to war and the right to conduct within a war. This is a largely philosophical concept but one that international law with regard to war often mirrors, references, or mimics. Further, policies and guidelines such as international law and just war theory place constraints on warfare and the warfighter such that they need to be understood before we explore how such policy-level restrictions manifest themselves as technical challenges in war and especially cyber warfare in later chapters.

Jus ad Bellum

The concept of the justice of war involves war being waged while respecting several constructs. There is having a cause that is just, for example, self-defense or defense of an ally. War must be conducted as a last resort to efforts such as diplomacy. A state going to war must do so with the appropriate authority, which in the case of the United States is with a declaration by Congress. The intent to go to war must be just and not self-serving, for instance, the annexation of Crimea could by some be viewed as self-serving and unjust, though, philosophically speaking, many Russians presumably view the activity as just or choose to not acknowledge as a state action of war. A war should only be started with a reasonable chance at success and be proportionate to the way it is waged.

A lot of this concept is strongly philosophical and too subject to debate to be involved in the discussions of technical obstacles in cyber warfare. That being said, several do lend themselves well to influencing and shaping actions during war in the domain of cyber. For instance, being conducted under the proper authority is an easily provable and understood concept as we have specific constitutional references that

dictate how war may be declared. We also have various titles of the US Code which dictate that activity such as cyber warfare must happen under appropriate authorities itself. Intention can certainly be framed in cyber, specifically as it is in wider warfare. For instance, using cyber warfare to steal money from banks of other states for the sole purpose of profit would certainly be understood to be with unjust intentions. A war should only be declared with a reasonable chance of success, and I believe that construct should aptly apply to the technical aspects of cyber warfare. For example, launching a computer worm which spreads from computer to computer that will destroy all the data on that computer but which has only a 2% chance of targeting the machines whose data you need destroyed might be viewed as having little chance of success. Avoiding the use of cyber warfare in such situations certainly keeps the activity more on the side of just than not based on the likelihood of success and prevents those uninvolved in the conflict from facing its affects.

Jus in Bello

The concept of just actions while at war is based on the two principles of discrimination and proportionality. Essentially the reason for differentiating between *jus ad bellum*, the justice of going to war, and *jus in bello*, justice while conducting warfare, is to diverge the cause of the conflict from the actions within it. It may, for instance, be viewed as just for the United States to declare war against the Empire of Japan after Pearl Harbor. Conversely, actions during that war, for instance, the nuclear bombings of Hiroshima and Nagasaki, are polarizing actions viewed by some as just and by others as unjust.

Using the nuclear bombing example, let's explore the event while looking at it through the lens of jus in bello—was it a just or unjust action while being within a just war? Using the concept of discrimination, it would seem that the action was almost certainly unjust. Any offensive action must be carried out in a way that discriminates between combatants and innocents. The bombings certainly could not and did not do this, and many innocent lives were lost in both bombings. When looked at from the second perspective of just warfare, that actions should be proportionate to the desired objective, it becomes a much fuzzier decision.

Though indiscriminate, the proportion of deaths caused by the bombings compared to the deaths that would have happened on both sides during the rest of the island warfare being carried out on Japan and nearby areas favors the bombings and resulting surrenders. This is likely true of both combatant and non-combatant deaths on the side

of the Japanese and certainly for combatants on the allied side. Through this lens it may be viewed as a just action within a just war, and certainly the decision makers who opted for the bombing must have felt so.

Just warfare has a large impact on the way cyber warfare should be carried out. Discrimination is extremely important given the interconnected nature of the cyber warfighting domain. We must ensure that if we carry out cyber warfare, we are able to have our offensive actions discriminate between combatants and non-combatants and even between targets within the declared enemy state and those without. In other warfighting domains such as air, land, and sea, it is not very likely that we accidently invade an ally, an abstainer, or even perhaps our own country.

Within the domain of cyber however, it can be extremely challenging to limit targeting to a specific enemy state while avoiding the occurrence of the effect acting upon a non-combatant or even a different nation state's asset. Let's take, for example, the Stuxnet virus, which almost certainly targeted the country of Iran and is largely heralded as an act of cyber warfare. Even in this advanced and very specifically targeted malware deployment, infections happened across the globe in many countries and in varying amounts. Certainly, all of the countries infected were not the target, and some were likely even allies to those which deployed the virus.

Proportionality is an extremely challenging constraint on cyber warfare as well. Take, for example, a cyber warfare offensive action that will shut down the power to the cyber-attack assets of another country. That in itself is certainly viewable as a just action of cyber warfare. But what if that same virus coincidentally also shut down the power to all the hospitals, traffic control systems, and water treatment plants of the target state. The objective of this action was to turn off the power to the cyber-attack assets of the enemy state; however, the result of the action would be considered in no way proportionate to that goal and would then be unjust. Once a cyber-attack has been launched, it can oftentimes be nearly impossible to cancel or reign back in and retarget completely. If the computers were shut down, it certainly can't be reversed or undone.

Many of the technical challenges discussed later in this book will hinge on these concepts to show how they impact war in general. Any state should strive in conducting cyber warfare to be as discriminate and proportionate as possible with the targeting of the offensive effects. When carried out successfully, such effects are a part of just warfare in a just war as illustrated in Figure 1-1. This must be done within the war such that the war can be declared justly and the actions within it, whether in the domain of cyber, land, air, space, or sea, can still be considered just themselves.