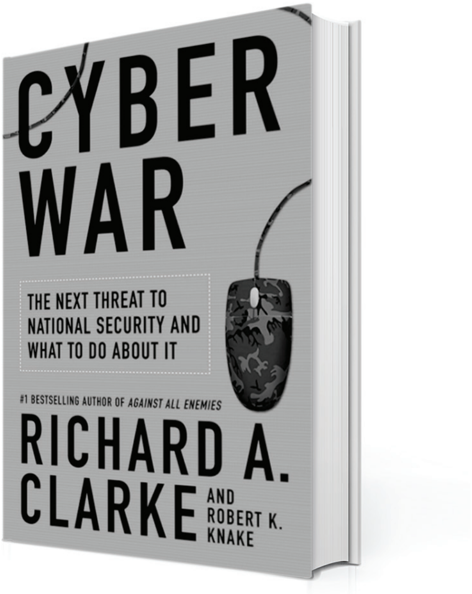
Cyber War
by Richard A. Clarke and Robert K. Knake

Reviewed by Professor Chris Arney and Second Lieutenant Joseph Kozlak



This book takes a holistic view of the cyber world and how it pertains to the United States regarding capabilities, vulnerabilities, policy, and potential strategies. We, as student and instructor in a course entitled *Networks for Cyber Operations* used this book as one of our texts in the Spring semester of 2016. Author Richard Clarke uses his experience in dealing with nuclear weapons, and his role as a Special Advisor to the President for Cyber Security to explain how the world situation has changed to make cyberattacks a significant threat to the United States. Clarke and Knake do an excellent job of speaking to a general audience (from cyber novices to experienced cyber warriors and hackers). The authors introduce the subject by describing the Israeli cyberattack on Syria before the bombing of a nuclear facility in 2007. This book stays away from the technical aspects of cyberattacks, but provides detailed background information about the Internet and how digitization has created a new battlefield.

Chapter 1, *Trial Runs* dives into how cyber disturbances in network capabilities such as crashing specific websites can be a precursor to the use of kinetic force. This chapter sets the background for how cyber war has been conducted in the past and illustrates some potential vulnerabilities for future attacks. The authors suggest there is a "credible possibility that such conflict may have the potential to change the world military balance and thereby fundamentally alter political and economic relations." (p. 53) This is the nature of conflict now, instead of a precision-guided munition targeting a specific area, a cyberattack can cripple an entire nation. Clarke describes in Chapter 2 how cyber units and systems are structured in the United States, Russia, and China. This sets the tone for his future discussion on the United States' cyber policy of the future. Chapter 3, *Battle Space* was our favorite as it detailed the variety of different elements that hackers' target. Clarke's explanation of the Trojan horse in a historical context was helpful in seeinghow vulnerabilities are exploited in the cyber world. It is easy for a code writer to add a couple of lines of code to software that can act as a logic bomb or the Trojan horse in the Internet. Furthermore, as society, especially commercial businesses, become more and more dependent on the Internet, there is a greater probability of someone becoming a victim of a catastrophic cyberattack. The need for cyber defense has grown with digitization, but how to build that defense is the vexing question of today.

Resilient defense of our networks is nearly impossible, and the ability to reliably and effectively retaliate is problematic because of the attribution challenge. Clarke uses the metaphor of an art thief and a hacker: "The difference between art thieves and world-class hackers is that with the best of the cyber thieves, you never know you were a victim." (p. 162) This is the issue that makes cyber defense so difficult, we do not know how or what a hacker is going to target, and when they do attack, we do not necessarily have alarms that sound. The hackers may leave with mountains of information yet not knowing if they stole any of it because we also have possession. If we cannot protect everything, we must protect our most valuable networks. But how we do that is still the question. The authors write with candor and strong opinions making the subject come to life for the reader.

After Clarke and Knake provide the background of attacks, hackers, and the vulnerabilities in cyberspace, they dive into explaining the creation of policies to deal with cyber operations. Clarke discusses the creation of a Defensive Triad. His background in Cold War politics dealing with nuclear weapons factors into this triad proposal. Cyber is different than the nuclear weapons of Cold War deterrence because cyber deterrence does not happen the same way. For one thing, if you do not use your cyber weapons periodically, no one will know or think you have the capabilities. Clarke discusses a practical illustration of cyber war, which is useful for readers interested in the future possibilities of cyber warfare. This chapter takes a step-by-step approach to explaining the different aspects and consequences of cyber war with a nation like China. Powerful nations have not gone to war with each other since World War II because of the deterrence of the lethal capabilities that such nations' possess, but now war can take place on the new cyberspace battlefield in which soldiers are not in direct combat. Finally, Clarke proposes his agenda to secure our systems and deter other nation states from attacking our networks.

Cyber War is a non-technical read that gives valuable insight into past, current, and future cyber situations and capabilities. The strength of this book is that it offers something meaningful for every reader. Clarke's stories add to the book's excitement by applying context to his theories of cyber operations. He adds valuable insight because of his background. This book is a call for action because the US government has been so focused on the wars in Iraq and Afghanistan that nations such as Russian and China may have moved ahead of the United States in the cyber domain. This is an excellent book for anyone looking to learn more about cyber capabilities and cyber policies in the United States.

Cyber War

Author: Richard A. Clarke and Robert K. Knake
Publisher: Harper Collins e-books, 2010
e-book: 351 pages
Language: English
ISBN: 978-0-061-99239-1

Chris Arney is a Professor of Mathematics at the United States Military Academy and former Head of the Department of Mathematical Sciences. He holds a Ph.D. in Mathematics and M.S. Degrees in Computer Science and Mathematics from Rensselaer Polytechnic Institute. He also holds a B.S. from the United States Military Academy. A career Military Intelligence officer, he served in tactical assignments, teaching assignments at USMA, and research positions at NASA Langley Research Center and the Army Research Office. His current research includes cooperative game theory, applications of network science, and mathematical applications to cyberspace.

Second Lieutenant Joseph Kozlak is currently assigned to 2-11 Infantry Regiment at Fort Benning, GA for Infantry Basic Officer Leadership Course. His follow on assignment is 3rd Brigade, 2nd Infantry Division at Fort Lewis, WA. Prior to commissioning in 2016, he received a B.S. with honors in Mathematical Sciences from the United States Military Academy. He was a four-year letter winner and two-year captain in hockey at USMA.

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.