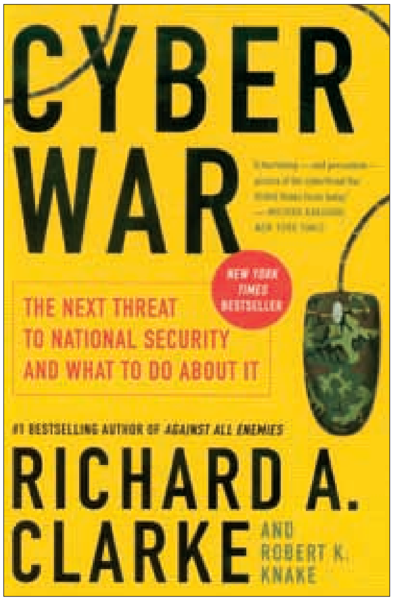
Book Review


CYBER WAR
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
NEW YORK TIMES BESTSELLER
#1 BESTSELLING AUTHOR OF AGAINST ALL ENEMIES
RICHARD A. CLARKE
AND ROBERT K. KNAKE

Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, HarperCollins Publishers, 2010, 290 pages.

by **Brandon Koh**

Cyber war is a very real threat to our modern day society. The definition of cyber war is "the use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems." Cyber war is not a victimless, clean kind of war that we should embrace in contrast to conventional forms of warfare. The public, civilian population as well as the privately owned corporations that run and own a country's key national systems is those that will suffer horribly from the aftereffects of a cyber war.

Clarke's writing is based on the United States (US) and how cyber war is a huge threat to US national security. He clearly defines what a cyber war is and how it might take place in the States, as well as the aftermath of such. Due to Clarke's background, he discusses mainly about the policies that the US should adopt going forward into preparation or to avoid a cyber war altogether.

Clarke in his first chapter, "Trial Runs," gives a brief history lesson or recap of how in the past, countries like North Korea and Russia have experimented with cyber warfare.[1] He explains that there are five takeaways from all these incidents, that cyber war is real, happens at the speed of light, is global, skips the battlefield and that it has already begun.[2] He also states that he believes that almost any actual wars in the future will be accompanied with cyber warfare as well, further highlighting the severity of the problem.

Clarke's bottom line in writing the book was that the US is not well prepared for a cyber war at all. He feels that the US will require sweeping new laws, regulations and policies in order to protect itself from this new and upcoming threat. He shows how other countries like China have fairly well prepared and strong cyber warriors.[3] In the case of the US, Clarke points out that the commercial side of networks is not well protected, and this is because they themselves do not want cyber protection by the government. This is enough reason for Clarke to propose that serious actions and measures must be taken to ensure cyber security in the US, and hence he proposes the Defense Triad Strategy.[4] Clarke goes on to talk about how the US should impose fundamental and structural changes to its system to adopt a defensive strategy.

Clarke also talks about offensive strategies the US can adopt and attempted to transfer strategies previously used in other conventional warfare into usage in cyber warfare. From Exercise South China Sea, a hypothetical exercise made by Clarke based on the 1983 movie about computers and war: *War Games*, Clarke explores the offensive strategies that the US would employ when faced off with a superpower such as China in a cyber war.[5] Offensive strategies that were effective otherwise, like deterrence, were out of the question as they did not translate well into deterring cyber attacks from other countries.[6] Of course, this meant that new strategies had to be employed, which is an alarming fact and should serve as a wakeup call to the US.

Clarke moves on to talk about cyber peace and how measures currently in place to ensure cyber peace, such as arms control in cyberspace, are not entirely effective. Clarke explains that arms control is not valuable and can even be unhelpful when it is largely hortatory, or when the negotiation is seen as an end in itself or a platform for propaganda.[7] Clarke mentions that there are four ways in which the US is more vulnerable to cyber war than those nations that might use cyber weapons on them. The US has a greater dependency upon cyber-controlled systems, they have more of their essential national systems owned and operated by private enterprise companies and thus has such politically powerful owners and operators, and lastly how the US military itself is highly network centric and is thus extremely vulnerable to cyber attack.[8] Clarke toys with the idea of completely banning cyber weapons and therefore banning cyber war altogether, but such a concept has many implications and aftereffects, thus making it highly situational. Lastly, Clarke closes off with his idea of an agenda that the US can adopt in order to better its cyber security and keep its people and country safe from cyber war.

Clarke served in the White House for Presidents Ronald Reagan, George H. W. Bush, George W. Bush and Bill Clinton. He was appointed as National Coordinator for Security, Infrastructure Protection and Counterterrorism. Hence, his insightful comments and remarks are very well thought and his view on how cyber warfare is rising in America and will be grave issue in the future is both credible and believable. While reading the book, I was constantly amazed at the accuracy and intricacy of information being doled out by Clarke, and I would expect no less of someone of his background.

The book is actually very well structured and an easy to understand format. Though some of the principles and attack/defense patterns may be challenging for the uninitiated, Clarke does seek to explain many of the alien concepts and does a good job of setting the groundwork upon which much of the work is built. Being both informative yet engaging, there was never a dull moment reading the book. Clarke not only dishes out substantial facts and figures to strengthen his arguments and points, but at the same time constantly kept me entertained and interested to find out more by painting a vivid picture of the US and it's possible post apocalyptic outcomes if it does engage in an all out cyber war. His outcomes were chilling and enthralling to read, and yet always seemed believable, showing his expertise and knowledge regarding the subject matter. Clarke constantly poses thought provoking questions regarding the state of cyber warfare and questions the readiness of the US to handle such a threat. These questions kept me engaged and constantly thinking of how the US themselves should in turn be preparing to fight or defend against a cyber war. Clarke would offer us his alternatives or solutions at the end and his answers were always succinct, precise and satisfying.

For those not so keen on reading about the US government and their structure as well as policies that should be put in place regarding cyber warfare, Clarke also covers many of the commonly asked or thought about topics; such as "What really is a hacker? What is meant by the term "kinetic" with regards to warfare"? Such topics are also commonly asked by many and thus the book will also cater for light readers who are interested in learning more about cyber warfare and cyber wars. This book would also be a perfect fit for anyone who is concerned about what might happen to the US if an adversary decides to turn their lights out, take away their computers, cell phones, electronic toys, and destroy their financial systems and their military in less than a day. Despite focusing mainly on the US, such horrifying scenarios can also be applicable to Singapore if we are not vigilant in our cyber protection and defense. The book is a perfect fit for anyone who has concerns about a future cyber war outbreak in the US, or the world for that matter. The book serves as a reality check, both to the US and the world, that cyber wars are very dangerous, and very much real. If you are concerned about cyber attacks and the guarding of cyber space, I would definitely recommend this book to you.

In conclusion, I found *Cyber War: The Next Threat to National Security and What to Do About It* both eye-opening and thought provoking. The book does not reveal any amazing cyber secrets, but the way the applications and agenda of cyber war were explained and written kept me considering the possibilities and repercussions that a huge scale cyber war could bring to the entire world.

ENDNOTES

1. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (HarperCollins, 2010), 18 and 27.
2. Ibid., 31.
3. Ibid., 54.
4. Ibid., 160.
5. Ibid., 179.
6. Ibid., 189.
7. Ibid., 225.
8. Ibid., 228 and 227.