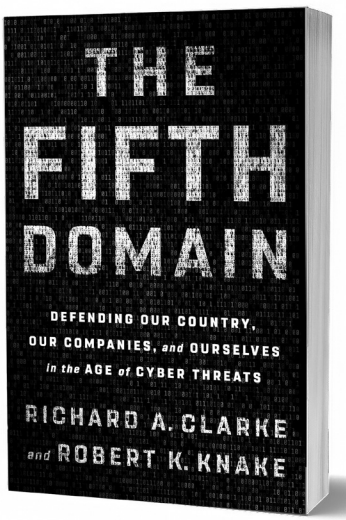
The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats



By Richard A. Clarke and Robert K. Knake

Reviewed by
Cadet Dylan Green

EXECUTIVE SUMMARY

Richard A. Clarke and Robert K. Knake's book *The Fifth Domain: Defending our Country, our Companies, and Ourselves in the Age of Cyber Threats* (2019) explains "why raising the alarm on cyber threats is warranted, and... lays out a plan for how the worst outcomes can be avoided."[1] Both Clarke and Knake provide unique perspectives on potential cyber threats as both have served as members of multiple presidential administrations' Department of Defense and Homeland Security staffs. Richard Clarke, in particular, "drafted the first national strategy on cybersecurity that any nation ever published."[2] With a foundational understanding of cyber policy implementation, both Clarke and Knake capitalize on their experience to create a superbly-crafted plan to reinforce corporations' cyber readiness, increase governmental focus and impact on cyber security, develop lasting and successful cyber policies, increase personal cyber security, and share their perspectives on critically important issues likely to surface in the near future. This review highlights Clarke and Knake's key assertions about establishing lasting cyber peace, and their views on implementing the proposed segmented plan.

1 Richard A. Clarke and Robert K. Knake, "The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats," Amazon (Penguin Press, 2020), https://www.amazon.com/Fifth-Domain-Defending-Companies-Ourselves/dp/052556196X, 15.

2 Ibid., 6.

CDT Dylan Green, is a Computer Science major at the United States Military Academy. He graduated from Northwood High School in Irvine, California, in 2020, and is currently performing undergraduate research in the Department of Electrical Engineering and Computer Science (EECS) and is a member of the Army West Point e-Sports team. He hopes to earn a master's degree in Computer Science through either the Lincoln Labs Fellowship Program or the National Science Foundation Graduate Research Fellowship Program before commissioning as a Cyber Officer in the U.S. Army.

It is worth noting that Knake and Clarke regularly refer back to their 2010 work, "*Cyber War: The Next Threat to National Security and What to do About It,*" and summarize some of the key ideas of that book, which, if read first, helps readers better conceptualize what is presented in *The Fifth Domain*. For those familiar with the US military, there also are references to military acronyms (e.g., the "OODA Loop" and "TTXs)," and institutions (e.g., West Point and Army Cyber Command). Clarke and Knake provide an invaluable overview of the greatest looming cyber threats and how best to implement cyber policy. In short, for cyberspace experts and novices alike, "The Fifth Domain'' provides a clear, in-depth, big-picture foundation to see our nation's path forward in this frontier.

Review

The Fifth Domain's readability distinguishes this book from most other titles in the genre. Despite hitting the market some three and a half years ago, the accuracy with which Clarke and Knake predict many issues that have become prevalent in recent times demonstrates the persisting value that this book has to offer. Additionally, the issues which have yet to come to fruition only further cements the necessity of continuing to reflect on this work. Clarke and Knake bring decades of experience at the highest levels of government to provide invaluable hypothetical and real-life examples on technical and policy issues for both novice and highly cyber-sophisticated readers. The book is broken into distinct sections, allowing for a clear understanding of their overarching cyber defense plan.

The first section, "**THE TWENTY-YEAR WAR**," lays out an excellent backdrop for this fifth (and only manufactured) domain, i.e., the "cyber domain," in which nations are rapidly competing for superiority. Clarke and Knake argue the US approach to the cyber domain is historically and fundamentally flawed due

to the overemphasis on developing offensive cyber capabilities. Rather than cyber offense, they advocate for cyber resiliency—the ability to side-step, blunt, and otherwise survive cyber-attacks with minimal damage. This would also make attacks on the US more costly, less effective, and potentially pivotal in achieving peace in the cyber domain. The authors acknowledge some irony in proclaiming their path to cyber peace, given their earlier book "Cyber War" (2010). Yet, they assure the reader that such a goal is entirely possible. They make specific recommendations for what actions corporations, the government, and individuals must take to achieve this goal.

Part two, "T**HE CORPORATE FRONTLINE,**" outlines what the authors view as the most important repository of responsibility for protecting our nation's cyberspace — corporations and the private sector. They underscore the responsibilities and behaviors businesses must be called upon to develop their cybersecurity and resilience capabilities. They discuss the uneven outcomes certain businesses can suffer with the same attacks, and one business can remain relatively unscathed while the other suffers major losses. The stark disparity in the quality of cyber security among companies critically undermines its value to the private sector. To remedy this systemic vulnerability, many basic changes must be internalized within corporate cyber security. To ensure overall security, the authors encourage the use of multidimensional and all-encompassing tools. They also urge universal standards for security tools and minimum standards to which all companies must adhere, along with the periodic public testing of tools, after and on top of internal lab testing—trust but verify. They view the implementation of cyber security minimums and opening businesses to public testing as attainable but observe that incentivizing cyber security companies to condense their software will be highly challenging, given the competing lucrative incentive to market multiple separate (and often redundant) products.

Part three, "**THE GOVERNMENT'S SUPPORTING ROLE**," discusses how the government can support the private sector through funding, basic laws, and the interplay between cyber security and the military. Clarke and Knake articulate clear and feasible methods for the government to support and improve cyber resilience. They argue that the most effective way for the government to increase general cyber security is through "nudges and shoves," by financially incentivizing companies that adopt certain cyber policies while withholding funds from those who do not implement these policies. The authors underscore the widespread distrust of government as to why the private sector should be the first and foremost responsible for cyber security, as it would be far more effective than trying to implement cyber security through government-run institutions. They argue that the government can and should support industry from behind the scenes. They additionally dedicate an entire chapter in this section to the US power grid, which remains vulnerable to cyber-attacks. They outline a five-step plan to secure the power grid, which requires direct cyber policy beyond mere governmental "nudges and shoves" and justifies this heavy-handed approach given the

dire consequences when a power grid is attacked. They urge the creation of a federal oversight agency to bolster the security of our power grids. They also flag the need to identify the existing back doors in the grids, add state-of-the-art cyber security, and create backup power grids for worst-case events. Their ultimate goal is to render US power grid security so airtight that potential aggressors question their ability to successfully launch an attack. In their detailed recommendations, the authors demonstrate a deep understanding of how the government and the general public process new policies and the politics of delivering an achievable, well-thought-out plan with minimal resistance from stakeholder parties.

Part four, "**WARRIOR DIPLOMATS AND CANDIDATES**," highlights the global interplay between government and the internet. They note that the many weapons in our cyber arsenal, with the lack of universally accepted rules on usage in this domain, render offensive deployment challenging and precedent-setting. They also note the absence of information flow between the US and its allies and how that impedes our collective ability to stop cyber threats from actors operating from other countries. To remedy this, they urge something akin to the EU's "Schengen Accord" to govern the internet, which allows freedom of movement through many European nations' borders. Rather than allowing countries to continue having their laws regarding cybercriminals, those participating nations would adhere to the same rules that govern individual conduct and law enforcement, such as access to shared databases. The authors acknowledge the political difficulties of such a regimen but conclude that to protect the very essence of democracy, the US must find a way to combat non-state actors who pose serious threats to democratic elections, which could be significantly facilitated by codifying a shared set of rules.

Sections five and six, "**THE (NEAR) FUTURE IN CYBERSPACE**" and "**YOU AND THE WAY AHEAD**," close out the book by describing the future of cyber warfare and laying out actions that we as individuals must take to exercise prudent individual cyber security. They include discussing some of the new and fast-evolving frontiers of cyber combat, i.e., artificial intelligence (AI), Quantum Computing, and 5G. These technologies are revolutionizing cyberspace. The authors conclude their book with takeaway lessons for all, i.e., the individual cyber security practices everyone should actively focus on daily. They reiterate that a lack of personal security has more far-reaching impacts than just the individual, and why effective resilience mandates the periodic backing up of key information and vigilantly ensuring that apps are not unwittingly allowed unnecessary access, and other basic cyber hygiene that lends itself to prudent defense and resilience in cyberspace.

Ultimately, *The Fifth Domain* outlines a coherent, cohesive, and executable plan to strengthen our country's cyber resilience. Some of their proposed corporate cyber policies may be challenging, as they may require businesses to forgo altruistically short-term profits and produce fewer but more comprehensive products. If these corporate changes were implemented, they would measurably improve national cyber security and lead to multiple long-term

benefits (and perhaps even include profits). And, unlike many alarmist books without foundation, these two authors cover an amazing array of issues, including glaring vulnerabilities, while providing an equally sound range of solutions. Clarke and Knake's depth of knowledge and ability to translate complex concepts in simple ways make "*The Fifth Domain"* an essential book that continues to be important not only for individuals not schooled in the intricacies of the cyber battlespace but for seasoned cyber warriors as well.

Title: ***The Fifth Domain: Defending our Country, our Companies, and Ourselves in the Age of Cyber Threats***

Authors: By Richard A. Clarke and Robert K. Knake

Publisher: Penguin Books (July 16, 2019)

eBook: 351 pages Language: English

ISBN: 052556196X

Price: $12.99 (eBook)