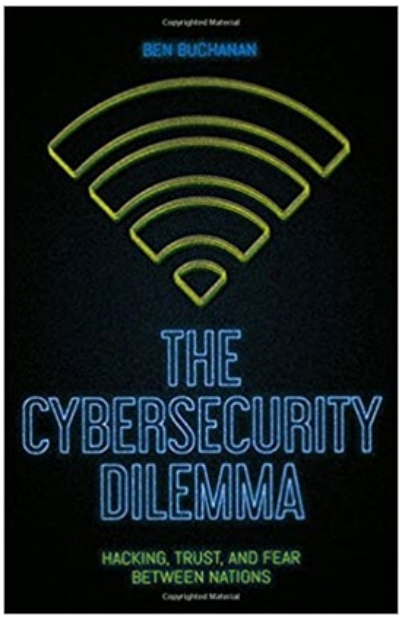
Journal of Military and Strategic Studies

VOLUME 20, ISSUE 4



Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. New York, NY: Oxford University Press, 2016.

Mark Peters, Technica Corporation

For now and the future, cyber security challenges remain central to state conflicts from small discussions to continent-spanning disagreements. The cyber perspective's analytical key to these discussions deciphers the motivation for how nations act across the Global Cyber Commons (GCC). Ben Buchanan, in *The Cybersecurity Dilemma:*

ISSN : 1488-559X

Hacking, Trust, and Fear Between Nations, codifies how, and why, cyber security challenges differ from more traditional national struggles while providing a format for future analysis. Excellent overall, the book delivers high-level perspectives, covers offensive and defensive network basics, and avoids derailing into detailed technical discussions. After establishing sound foundations, Buchanan next demonstrates the appropriate lens for cyber security problems and associated mitigations. *The Cybersecurity Dilemma* coherently packages much-needed insight into one of today's most challenging areas. Anyone whose professional or personal concerns deal with cyber security should immediately pick up a copy. Well researched and smoothly written, this text makes a valuable, and needed, addition to any strategist's shelf.

The Cybersecurity Dilemma intellectually hits the mark chapter after chapter. The book includes few figures while mostly featuring well sourced textual arguments, extensive end notes, and a full bibliography. The material starts out evaluating the core security dilemma concept while exploring network attackers' and defenders' viewpoints. Each element advances solidly as Buchanan expands from traditional shortfalls to cyber security's contributions to a new strategic model as shown below:

> It is here that the mitigators' paradigm breaks down when applied to the cybersecurity dilemma. That paradigm relies on the widely shared notion that offensive technologies are threatening and defensive ones are much less so. As the previous chapter shows, however, while some intrusions are not offensive, they are still nonetheless threatening, for a variety of reasons. Even if a state has managed to conclude that a particular intrusion is solely defensive in nature- something that it is unlikely to do authoritatively-the presence of a potential adversary in the network still poses a threat for the future. Indeed, the intrusion is threating in a variety of ways that the traditional defensive technologies envisioned by mitigators, such as mines and fortifications, simply are not (113).

The author's careful textual integration between previous studies, new material, and evolving viewpoints allows the reader to smoothly follow the explanations. Experienced researchers may benefit more but the skillful integration overall makes the presented material widely accessible.

Buchanan's core belief advocates for cyber security events as substantially different from traditional state-based interactions. The work compares cyber aspects to

more familiar interactions in order to propose three cyber security dilemma pillars. The first pillar states cyber operations begin well before crisis events with lengthy access preparations prior to any attack. Like a burglar, network attackers must first find a network path, with more careful planning decreasing detection risk. The second pillar suggests actors believe defensive reasons justify attacks against other state's networks. Cyber space's flexible nature allows states to steal data, and cripple network defenses when a defensive kinetic attack is unlikely. For example, despite crippling the US Pacific Fleet, no one views WWII's Pearl Harbor bombing by Japan as defensive in nature. Finally, the third pillar explains states view all intrusions against important networks as threatening. These three pillars create the cyber security dilemma framework for potential escalations and subsequent responses. After establishing the model, the book examines traditional network perspectives, discusses cyber security dilemma changes, and considers counterarguments.

Much like other genre examples, *The Cybersecurity Dilemma* begins with the author's perceptions on offensive, defensive, and intelligence-based cyber space actions.[1] Each section features a light sprinkling of historic examples demonstrating central points. Offense, for Buchanan, highlights several foundational factors; cyber operational speeds vary, momentum does not build to reach what Jomini would consider a classic tipping point, persistence is powerful, and operations are designed in advance. These factors support the first pillar's consensus that cyber operations are planned well before any crisis.

The defensive exposition connects network protection to counterintelligence by reasoning all states must protect their networks, especially critical infrastructure, from data exfiltration as well as outright attack. Buchanan's network defense entails preparation, detection, collection, analysis, containment, and decontamination. These steps, however, reflect intrusion responses more than an initial network defense. Further, the text offers the opinion that detected intrusions help defenders through gaining perspective on an attacker's targets and techniques. These thoughts allow one to summarize the second pillar; states attack other state's networks to improve defenses,

[1] Several excellent examples include *Understanding Cyberwarfare* by Brian Mazanec and Christopher Whyte (2018), *Cyber War Will Not Take Place* by Thomas Rid (2013), or *Cyber War* by Richard A. Clarke and Robert Knake (2012).

not as inherently offensive actions. Successful intrusions scale from significant preparation to very little. Those polar opposites link four actor motivations; countering specific threats, shaping future conflicts, establishing persistent beachheads, or posing counterintelligence challenges. Intrusions shape the third pillar as activity against important networks appears threatening to all states. The author repeatedly illustrates how these pillars challenge states mired in traditional processes.

Perceptions can create subsequent reality and as each state shapes their reaction based on perceiving individual events across the GCC through their network defenses. Four elements distinguish cyber from traditional security dilemmas with the first as the offense-defense balance. Visually inspecting physically weapons allows one to easily perceive a quantitative or qualitative edge but deciding cyber space advantage can be more challenging. Those balances lead to the second element suggesting no cyber weapon is inherently offensive or defensive with many dual employment possibilities. The third element evaluated internal motivations based on material greed. States traditionally signal to other states through treaty agreements, policy, or unilateral restraint. Cyber-oriented actions, however, such as conducting espionage, increasing network defenses, or advocating certain international norms may be viewed as concealing rather than signaling to an opponent. The last element, unit analysis, links to motivation with those states with improved intelligence and analysis functions as less likely to war. As with greed, cyber action's granular intentions conceal better than reveal, so states conducting cyber-based actions may appear as verging on the attack during routine activity.

Exactly how intelligence and information distribution affects a state's decisions features as central to continuing discussions. The text argues cyber-based information is less specific, less complete, and less timely than traditional intelligence like imagery or signals intelligence products. These uncertainties suggest three possible cyber security dilemma limitations. The first limitation addresses attribution, which, while not impossible, can be difficult and frequently depends on how users employ data.[2] Second, cyber threats remain largely non-existential as no state will cease to exist from cyber

[2] An excellent recent summary on the problems with attribution and ways to specifically address those concerns can be found in Clement Guitton's *Inside the Enemy's Computer: Identifying Cyber Attackers* (New York, NY: Oxford University Press, 2017).

attacks. The last limitation holds that cyber power is unequally distributed and states will always fear cyber threats regardless of escalation but the lacking of either existential threat or reliable attribution means GCC-based attacks will have little to no impact on state actions. These limitations allow one to derive three areas to reduce threat exposure; implementing baseline defenses, advocating bilateral agreements, and securing system-wide security postures. Not surprisingly, these are the same factors states advocate when addressing security dilemmas. For example, one can evaluate present US policy as a standing military contributing to baseline defenses, advocating bilateral and multilateral agreements such as NATO, and improving overall security through varied measures.

The Cybersecurity Dilemma poses several excellent arguments with a wide variety of source material and incorporates a keen grasp of political strategies. The text's theoretical focus could use several more graphics or tables to illustrate discussions but does not suffer greatly from the shortfall. The dilemma pillars are a useful event interpretation schema but are not portrayed as a functional framework during this work. Examples were small, and somewhat dated. The mild dating likely relates from this review occurring four years after initial publication. The book's biggest shortfall remains the lack of any one case study or scenario to longitudinally discuss the cyber security dilemma from a state, or states, view. For example even using the BYZANTINE CANDOR events, Buchanan could have presented a chapter illustrating the various events and perspectives from multiple viewpoints.[3] Perhaps, the author can take the idea for applied pillars with fully developed case studies for a future text.

Overall, the concepts and discussion Ben Buchanan presents throughout *The Cybersecurity Dilemma* are innovative and make it a must read for any international strategy enthusiast. Basic technological background is covered quickly and well-coordinated with the more advanced material later in the book. The subject matter delivers in multiple areas through comparing the cyber security dilemma to more traditional challenges and comprehensively evaluating each. I previously examined this book from time to time as a potential read and honestly regret not having picked it up

[3] BYZANTINE CANDOR refers to Chinese efforts to hack US defense contractors. See Nicholas Sambulak, *Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology* (Santa Barbara, CA: ABC-CLIO, 2019), p. 70.

before now. This well-rounded, exhaustively argued, and intriguing book should be added to every political strategist's shelf.

Dr. Peters served 22 years as an intelligence officer with the US Air Force. Familiar with strategy and operations across a variety of levels, he specialized in space and cyber applications including commanding a space intelligence squadron. He is the author of Cashing in on Cyberpower, examining over 10 years of cyber attacks for their economic impacts. Holding degrees from the US Air Force Academy, Troy University, and Henley Putnam University, he currently works as Cybersecurity expert for Technica Corporation as a defense contractor supporting USAF cyber weapon systems.