Journal of Strategic Security

Volume 12 | Number 3 Article 6

Understanding Cyber Warfare: Politics, Policy and Strategy By Christopher Whyte and Brian Mazanec. New York: Oxford University Press, 2017.

Mark T. Peters II
USAF, Retired

Recommended Citation
Peters II, Mark T.. "Understanding Cyber Warfare: Politics, Policy and Strategy By Christopher Whyte and Brian Mazanec. New York: Oxford University Press, 2017.." *Journal of Strategic Security* 12, no. 3 (2019) : 175-178.
DOI: https://doi.org/10.5038/1944-0472.12.3.1765
Available at: https://scholarcommons.usf.edu/jss/vol12/iss3/6

Understanding Cyber Warfare: Politics, Policy and Strategy By Christopher Whyte and Brian Mazanec. New York: Oxford University Press, 2017.

Understanding Cyber Warfare: Politics, Policy and Strategy By Christopher Whyte and Brian Mazanec. New York: Oxford University Press, 2017. ISBN 978184905544. Pp. 304.

International relations, business, and policy professionals often share complaints about how cyberspace's dynamic nature impedes their ability to choose effective actions. Whyte and Mazanec make significant inroads towards increasing basic and advanced cyber warfare knowledge in their new textbook, "*Understanding Cyber Warfare: Politics, Policy, and Strategy.*" Those new to the field, or simply requiring a refresher, will find the first several chapters about network functionality and some elementary cyber operations strategy provide a solid basis. The topics swiftly advance through foundational and recent history before using current lessons learned to advance theory considerations. These theories incorporate varied state and non-state activities while suggesting potential governance strategies and forthcoming changes. Throughout the entire text, call-out boxes reinforce central messaging, a glossary contains new terms, and selections for future reading guide additional research. Overall, the textbook makes an excellent addition to either political or technical instruction discussing cyber events and it makes an excellent reference for current cyber operators.

As with most superior textbooks, Whyte and Mazanec's teaching relies on building out from the basics to the truly advanced topics. The book's theme expresses that Information Communication Technology (ICT) has changed the world and subsequently altered international relations processes, and that understanding processes across the new model is critical. The incremental learning process allows students at all levels to progressively build knowledge, or to skip ahead to relevant sections. The first several chapters review the cyberspace environment's basics and roughly sketch an existing international relations process. Next, discussion veers to operational vectors concerning exploitation and attack processes. Having established a sound theoretical foundation, the next step reviews state and non-state actors as well as how cyber activities typically occur in gray, not-war actions. The historical summaries lead to the book's final section, discussing where cyber-warfare strategy may progress through unique national experiences, the potential for adopted norms, and a glimpse at possible futures.

Cyberspace often intimidates new students by the technical debt volume incurred when first contemplating this arena. The textbook alleviates this issue by beginning with standardized processes and terminology. The first chapter's overview describes the Internet's emergence, technical construction, and security standards employed. This then moves on to cyberspace's global concerns by discussing political schools such as realism, liberalism, and constructivism. After some scene setting, the next two chapters discuss cyber warriors operating through environment discovery, exploitation, and attack. Notable discussions here include a quick look at how intelligence collection practices changed following the 9/11 attacks as well as the hack-back operational strategy. Hack-back concerns are central to many cyber-security discussions through everything from a need for effective attribution standards to how much of a response state or non-state actors may undertake in their defense.

The middle section of the book summarizes historical cyber actions and cyber processes before progressing into the book's two best chapters on cyber conflict as "not war" and non-state actors. The historical overview lists fourteen major cyberspace actions including Stuxnet, Operation Ababil and Moonlight Maze. These actions should be mostly familiar to cyber professionals but Black Energy's Ukrainian SCADA attacks and North Korea's Sony hack are useful additions. Having reviewed these useful cases, Whyte and Mazanec use arguments about power, protection, and deterrence models to examine why states pursue cyberwar. The "not war" chapter expands the overall cyber parameters by connecting emerging information war possibilities with gray zone conflict considerations. Those changes are followed by an exhaustive non-state actor discussion with how cyber activities influence terrorism, social activism, and proxy fights. If nothing else, the mobilization, mitigation, and actualization triangle modeled by subversive campaigns and social activist scaffolding should be critical reading for any cyberspace student. The authors' skills also emerge when combining those activist aspects emerging from terrorist and criminal actions as indicative of overall cyberspace risks. As always, the text notes that even when winning a cyber-action, effects may only last as long as the next reboot or patch. This leaves the keys to cyberspace victory in changing user perspective as much as altering electronic functions.

Finally, the text explored national policy perspectives, emerging international standards, and where future cyber conflicts may venture. The national section discusses not just U.S. but also UK and NATO policies as Western examples, while introducing students to some regions frequently seen as aggressors, including Chinese, Russian, Iranian and North Korean policies. Both this chapter and the norms discussion serve as the textbook's advanced study portions. The norms section draws heavily on Mazanec's own publications while adding material describing further development and behavioral modifications emerging from desired cyber norms. Several examples where norms may change current behaviors include collateral damage responsibilities resulting from cyber actions or cyber-weaponry restrictions similar to nuclear or chemical weapon treaties. As a last stop, the text mentions potential future topics including the nearly mandatory topics of cloud computing and artificial intelligence as well as how the Internet of Things significantly increases attack surfaces for all global citizens.

As a textbook, *Understanding Cyber Warfare* deserves a high rating, but several potential improvement areas exist. For any second edition, or simply online additions, including an overall instruction outline more specifically organizing the relationships between chapters, thought questions for the material, and more graphical explanations would all be helpful. While all the instruction does fall into a roughly organized structure, providing the authors' direction for integrating other potential topics would likewise be useful. Continuing a similar theme, as the textbook seems intended for the classroom, discussion topics at each chapter's end would be beneficial. Some graphics do appear; however, a larger table and diagram selection could improve the text as existing images are concentrated in the Attack, States, and Norm chapters rather than distributed across the text. The majority of the examined material was compiled from existing sources rather than advancing new research as might be expected from such a work.

Overall, Mazanec and Whyte are on target across all the required functions for cyber success and join a handful of other excellent cyber textbooks including *Understanding Cyber Conflict: 14 Analogies* (Perkovich and Levite), *Cybersecurity Ethics* (Manjikian), *Cybersecurity and Cyberwar* (Singer and Friedman). *Understanding Cyber Warfare: Politics, Policy and Strategy* includes a glossary and further reading suggestions for each chapter. The two authors each clearly made use of their individual talents, linking learning topics to other well-known and accredited individuals in the area including Thomas Rid, Nazli Choucri, Jason Healy and many others. All cyber operators and planners should consider this volume as an extremely useful desk reference and those new to the field should consider themselves well served when taking a class requiring this text.

Mark T. Peters II, USAF, Retired

DOI: https://doi.org/10.5038/1944-0472.12.3.1765