Journal of Strategic Security

Volume 7
Number 1 *Volume 7, No. 1: Spring 2014*

Article 8

Conflict and Cooperation in Cyberspace: The Challenge to National Security. Edited by Panayotis A. Yannakogeoros and Adam B. Lowther. Boca Raton, FL: Taylor and Francis Group, 2014.

Mark Roberts
Security Consultant

pp. 83-84

Recommended Citation
Roberts, Mark. "Conflict and Cooperation in Cyberspace: The Challenge to National Security. Edited by Panayotis A. Yannakogeoros and Adam B. Lowther. Boca Raton, FL: Taylor and Francis Group, 2014.." *Journal of Strategic Security* 7, no. 1 (2013) : 83-84.
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.7
Available at: https://digitalcommons.usf.edu/jss/vol7/iss1/8

Conflict and Cooperation in Cyberspace: The Challenge to National Security. Edited by Panayotis A. Yannakogeoros and Adam B. Lowther. Boca Raton, FL: Taylor and Francis Group, 2014.

Abstract

Conflict and Cooperation in Cyberspace: The Challenge to National Security. Edited by Panayotis A. Yannakogeoros and Adam B. Lowther. Boca Raton, FL: Taylor and Francis Group, 2014. ISBN 978-1-4665-9201-8. Tables. Figures. Sources cited. Index. Pp. xxviii, 332.

***Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Edited by Panayotis A. Yannakogeoros and Adam B. Lowther. Boca Raton, FL: Taylor and Francis Group, 2014. ISBN 978-1-4665-9201-8. Tables. Figures. Sources cited. Index. Pp. xxviii, 332. $59.95.**

The range and complexity of modern security dilemmas are myriad: terrorism, identity theft, fiscal instability, and international relations, to name a few. Landing front and center is the relatively new cyber realm that has yet to be defined, yet demands some form of structure. In this wide-ranging anthology that encompasses expert viewpoints from military, civilian, and private sector contributors, the editors seek to provide a broad framework of issues to be considered. Rather than provide definitive answers (all of the contributors readily admit that none exist), the contributors state that in order to attain the right answers, we must first ask the right questions. Over the course of the book, the authors put forth a common set of concerns to frame the issue at hand.

The cyber domain is one that is still developing and the writers examine this new paradigm through the prism of how to collect information or prevent it, depending on the national security viewpoint. The cyber field encompasses commerce, diplomacy, social networking, governmental monitoring, military systems, academia, and information propaganda, to name but a few. Viewed within this context, cyber is an anti-U.S. tool that rogue nations, criminal networks, and terrorists have at their disposal. Conversely, the U.S. can also use that same tool against its adversaries.

Woven throughout these dilemmas are the complex legal frameworks that accompany cyber policy and strategy. The U.S. Government and its intelligence and military infrastructure must also work alongside private industry (who owns over 80% of America's critical infrastructure) on the difficult issues of how to develop legal and policy solutions to protect the nation in cyberspace. At the same time, legal complications arise when trying to define how to limit government and regulatory interference in a privately owned and operated domain, while trying to protect it from cyber criminals. Thus far, the U.S. Air Force (USAF) has been on the cutting edge of cyber doctrine and has made the most progress in defining "the way ahead" for cyber doctrine.

Within this framework, the authors recommend a national and international effort to develop common cyber definitions and lexicon. In so doing, all parties involved would have a standardized framework within which to proceed (at present there are many definitions of "cyberspace," all of them contingent on the organization defining them). As cyberspace is part of the nation's critical infrastructure, it takes on added importance in how to protect and defend it. As a military weapon, it is part of the warfighting domain as well.

All authors agree that the U.S. needs to understand rapidly developing and evolving cyber technologies in order to solve the accompanying security challenges confronting the nation. Early software and hardware designers had no way of envisioning today's interconnected world, or the legal and commercial issues that would issue forth in a universe populated by hackers, viruses, bugs, and cyber criminals. The Department of Defense (DoD) has statutory limitations imposed on it that impact DoD capabilities and operations. Cyber is such a new frontier that it

becomes problematic to devise a policy for a problem that is difficult to define and evolves on a daily basis.

The authors ask how the U.S. can hold other nations accountable if it can't even define or codify its own policies? The authors call for international cyber agreements, but admit that such agreements are not technically feasible or enforceable under international law. The closest ide that approaches this concept is a framework by the U.S. Government to build a set of cyber standards based on digital policy management capability intended for the DoD. The USAF role in cyber security has been to generate programs, processes, dissemination protocols, and storage and destruction guidelines. Even with all of this activity, the relationship between government and industry is uneasy at best, as their interests are not always mutual.

The authors examine how to employ cyber capabilities offensively to further U.S. national security policy, admitting that without buy in from international partners, this has inherent risks with a high possibility and even probability of backfiring. The authors recommend that the U.S. seek international agreements to limit and outlaw the damaging effects of terrorist and criminal actions on international industry, trade, commerce, and communications.

The authors undertake a study of how to apply cyber law to cyber war, warning that allowing the Intelligence Community and the military to assist in the defense of privately owned networks may lead to legal and political consequences. They also grapple with the environmental aspects of cyber: a cyber-attack against an industrial control system (energy, nuclear, chemical, or waste management), would lead to massive environmental damage, staggering economic losses, and cause (potentially) rampant public health hazards.

This well-written tome brings together a cast of eminent thinkers, military strategists, academics, cyber specialist, and policy experts to examine cyber challenges for U.S. and international diplomats and decision makers. While it keeps its emphasis on policy-relevant solutions, it maintains the need for a common core of concepts to better define, codify, and approach this new concept that will be with us for years to come. It main utility is in the questions raised, vice answers provided. The book would be of most use for those attempting to better understand cyberspace and possible policy avenues for the future.

Mark Roberts, Security Consultant

https://digitalcommons.usf.edu/jss/vol7/iss1/8
DOI: http://dx.doi.org/10.5038/1944-0472.7.1.7