Why the United States Needs to Think of Cyber Security in a New Light

By The NATIONAL RESEARCH COUNCIL

Edited by William A. Owens, Kenneth W. Dam & Herbet S. Lin et al. eds.,

The National Academy Press, 2009, ISBN: 978-0-309-13850-5

Price: $49.99 pp. 390

Reviewed by Devin Woolf

Journal of High Technology Law

Suffolk University Law School

Keywords: Cyber Attacks, Cyber Security, Foreign Policy, Cyber Security Defense, Technological Warfare, National Security, Law Enforcement, United States, Ethics, Policy

---

"… [I]n September 1988, then-Russian foreign minister Igor Ivanov wrote to Kofi Annan, United Nations secretary-general, warning that the effect of information weapons 'may be comparable to that of weapons of mass destruction'" [1]

Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities produced by the National Research Council argues that cyber security should be placed in the hands of law enforcement and only the decision making and oversight should be left to the executive and legislative branches.[2] This book analyzes the challenges facing the U.S. in the new realm of cyber security and compiles policies governing other types of warfare, to

[1] NATIONAL RESEARCH COUNCIL, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 328 (William A. Owens, Kenneth W. Dam & Herbet S. Lin et al. eds., The National Academy Press, 2009).

[2] *See* National Research Council, *supra* note 1, at 328.

help form a cyber-security policy for the United States that is technologically and economically feasible. The authors suggest transferring cyber security preventive measures to the government but leaving the cyber defense capabilities to the hands of law enforcement agencies, keeping the decision making on whether to launch these attacks to the Executive Office and Congress.

The author of this work is The National Research Council. The National Research Council consists of members from the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.[3] For this particular publication, the Committee on Offensive Information Warfare, Computer Science and Telecommunications Board and the Division on Engineering and Physical Sciences all contributed to create the final product.[4]

The National Academy of Sciences ("NAS") is a private, not for profit society of distinguished scholars who have been elected by their peers for their outstanding contributions to research in the field of science.[5] An Act of Congress established the National Academy of Sciences in 1863.[6] The NAS provides independent advice to the nation on matters related to science and technology.[7] The National Academy of Engineering is part of the NAS founded in 1964 and works with the National Academies of Sciences, Engineering and Medicine.[8] These groups together provide independent objective analysis and advice to solve complex issues and inform public policy. [9] The third group within the NAS is the Institute of Medicine. [10] Federal Agencies and the private sector request research to help them make informed health decisions for

[3] *See* THE NATIONAL ACADEMY OF SCIENCES *archived at* https://perma.cc/HSM9-FSPY (last visited Feb. 3, 2016).
[4] *See* THE NATIONAL ACADEMY OF SCIENCES, *supra* note 3.
[5] *See* THE NATIONAL ACADEMY OF SCIENCES, *supra* note 3.
[6] *See* THE NATIONAL ACADEMY OF SCIENCES, *supra* note 3.
[7] *See* THE NATIONAL ACADEMY OF SCIENCES, *supra* note 3.
[8] *See* THE NATIONAL ACADEMY OF ENGINEERING, *archived at* https://perma.cc/3297-VGZQ (last visited Feb. 3, 2016).
[9] *See* THE NATIONAL ACADEMY OF ENGINEERING, *supra* note 8.
[10] *See* INSTITUTE OF MEDICINE, *archived at* https://perma.cc/X8Q9-2QAM (last visited Feb. 4, 2016).

the United States and private citizens. [11] The Institute of Medicine holds roundtable events, standing committees and conferences to allow for the discussion and critical thinking of those in the health and technology field. [12]

The other groups that participated in the creation of this work were the Committee on Offensive Information Warfare, which is a standing committee of the National Research Council.[13] The Committee first met in July of 2006 to discuss topics related to cyber-attacks. [14] The Computer Science and Telecommunications Board is part of the division on Engineering and Physics within the National Academy of Sciences. [15] Some of the recent publications from the Division on Engineering and Physical Sciences include; *Telecommunications Research and Engineering at the Communications Technology Laboratory of the Department of Commerce: Meeting the Nation's Telecommunications Needs*, the *Interim Report on 21st Century Cyber-Physical Systems Education*, *Future Directions for NSF Advanced Computing Infrastructure to Support U.S. Science and Engineering in 2017-2020: an Interim Report*.[16]

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities discusses cyber warfare both active and defensive strategies describing the basic technology used to carry out attacks and preventive measures, while posing ethical considerations for the use of such warfare.[17] The book provides the reader with an in depth summary of the capabilities of the United States and how the United States should decide to use its technologies in light of ethical considerations including international treaties. The book is

[11] *See* INSTITUTE OF MEDICINE, *supra* note 10.
[12] *See* INSTITUTE OF MEDICINE, *supra* note 10.
[13] *See* IT LAW WIKI, *archived at* https://perma.cc/4XMX-YUWL (last visited Feb. 4, 2016).
[14] *See* IT LAW WIKI, *supra* note 13.
[15] *See* Computer Science and Telecommunications Board: Division on Engineering and Physical Sciences, The National Academy of Sciences archived at: https://perma.cc/5NQ4-AJW2 (last visited Feb. 4, 2016).
[16] *See* Computer Science and Telecommunications Board: Division on Engineering and Physical Sciences, *supra* note 15.
[17] *See The National Committee of Sciences; supra* note 1.

broken down into three parts.[18] The first part includes the framing and basic technology of cyber-attacks and cyber exploitation and when each is used and for what purpose.[19] The beginning chapters focus on making a clear distinction between cyber-attacks and cyber exploitation.[20] The chapters go on to explain the basic technology behind both along with operational considerations.[21] The first part concludes with a brief overview of historical approaches to maintaining defensive and reactive cyber security.[22]

The second part discusses the goals of different agencies that have an interest in engaging in cyber defense or launching cyber-attacks and each of their objectives while comparing cyber defense and cyber-attacks to traditional uses of military force.[23] The second part presents the different perspectives for the usefulness of cyber exploitation and how the information gathered can be analyzed and of use to different intelligence agencies.[24] The second section discusses the ability to remove cyber security from the national security agenda for the most part and place it inside the use of law enforcement.[25] The second part concludes with the ability to oversee and make decisions on when to launch a cyber-attack and when to have cyber defenses in place that affect the national security of our country and how the executive and legislative branch could act as the branches of government to make decisions and oversee that cyber measures are carried out in accordance with law.[26]

[18] *See The National Committee of Sciences; supra* note 1.
[19] *See The National Committee of Sciences; supra* note 1, at 79-160.
[20] *See The National Committee of Sciences; supra* note 1, at 80-85.
[21] *See The National Committee of Sciences; supra* note 1, at 110-133.
[22] *See The National Committee of Sciences; supra* note 1, at 156-159.
[23] *See The National Committee of Sciences; supra* note 1, at 161-180.
[24] *See The National Committee of Sciences; supra* note 1, at 188-197.
[25] *See The National Committee of Sciences; supra* note 1, at 200-213.
[26] *See The National Committee of Sciences; supra* note 1, at 214-235.

The final part of the book discusses the legal and ethical considerations for cyber-attacks highlighting the many international treaties such as human rights law and how those perspectives should kept in mind when forming a United States policy.[27] The final part informs the reader of the rules governing nuclear, biological and non-lethal weapons and compares the different type s of war to the comparable destruction as a result of cyber warfare.[28] The third part of the book discusses the types of conflicts that could arise in the cyber arena and the politics that could be involved in such a conflict.[29] The book concludes with providing alternative perspectives and regulatory regimes for deciding and overseeing cyber-attacks and how foreign actors have approached their cyber security policies.[30]

Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities advocates for cyber security to be taken out of the national security context and placed in the hands of law enforcement with oversight and decision making capabilities still given to the executive and legislative branches by creating a feasible possible.[31] At first glance, giving law enforcement agencies the authority over cyber security can feel like removing a national security issue and placing it in ill-equipped hands. After realizing the positives of such a change and recognizing that the executive and legislative branch would still play a role in oversight and decision making, the National Academy of Sciences gives the reader confidence that their suggestions are feasible and best suited.

This book is intended for students and professors in the cyber intelligence and technology field. It is easy enough for an individual with not much knowledge of cyber security since it

[27] *See The National Committee of Sciences; supra* note 1, at 239 – 328.
[28] *See The National Committee of Sciences; supra* note 1, at 293-299.
[29] *See The National Committee of Sciences; supra* note 1, at 302-315.
[30] *See The National Committee of Sciences; supra* note 1, at 318-322.
[31] *See The National Committee of Sciences; supra* note 1.

spends the first few chapters describing in depth, the operations behind both cyber-attacks, cyber exploitation and cyber defense. Professors and academics also have a lot to gain from this book since it includes both domestic and international policies that are related to the field that should be kept in mind when deciding on a U.S. cyber security policy. The book is also a great source for lawyers who work in the field of cyber intelligence since it reminds lawyers to keep in mind ethical considerations so as not to violate international treaties and obligations.

The book is structured in an orderly format, which allows for optimal understanding. The beginning chapters describe in layman's terms the basics and fundamental differentiating cyber-attacks from cyber exploitation and the purpose and use of each. This from the beginning allows for clarity and a better understanding for the purposes and policies that should be set forth for both. By describing the historical perspectives of how policies have been created for similar areas of the law, the authors provide a basis for why such a policy would not work for cyber security or how similar policies can be utilized.

For a topic that may appear dry and complicated, the authors make the book a fairly easy read. Beginning with layman's explanations and progressing with technology language once the reader has a solid understanding of basic concepts is the perfect method to get readers to dive into the policies and the explanations behind historical legislation. The book becomes more fascinating as the chapters progress, making the reader feel informed in the area. At every new point in the book, the reader finds herself constantly thinking about the feasibility of each proposed policy and questioning how it could be done differently.

This book is a valuable contribution to the field of cyber security. It creates a feasible policy solution for better protecting the U.S. from cyber-attacks and exploitation and the ethics and policy to help decision makers make the choice of launching a cyber-attack on targeted parties and to the extent at which the attack will reach. The amount of information on the field of cyber security is more than ample for a student or academic to grasp an in-depth understanding of the complex and constantly changing area.

It must be kept in mind the book was created as a report which included all of the findings from the National Academy of Sciences, for the future, if college aged students could be reached out to, I think providing a more concise version of the research and solutions would be best suited in less complicated terms. For the audience it was intended for, such as the federal government and scholars in the field, it was the perfect combination of technical language that was somewhat easy to comprehend.

After reading this work, I would recommend it to others in the field of cyber security. With all of the research cited and provided, it is hard not to be convinced of the Committee's suggestions. The work was incredibly informative and makes the reader feel as if the government is more educated in the area of cyber security than the average person would realize. In the future I would read other reports published by the committee because of the amount of information is