Review - Cybersecurity and Cyberwar

https://www.e-ir.info/2014/01/06/review-cybersecurity-and-cyberwar/

ALEX STARK, JAN 6 2014

Cybersecurity and Cyberwar: What Everyone Needs to Know
By: P. W. Singer and Allan Friedman
New York: Oxford University Press, 2014

The year 2013 saw a number of headline news stories featuring a variety of different actors and sectors, but all with their roots in the same place: the cyber world. Edward Snowden disclosed a series of classified NSA documents detailing the United States' global surveillance apparatus, including Internet surveillance programs like PRISM. The US federal government launched the website healthcare.gov to facilitate enrollment in health care exchanges, and an acting assistant secretary of Homeland Security testified before congress in November that the site experienced a series of attempted hacks. Conspirators who hacked into the systems of Nasdaq, Visa, and J.C. Penney and other major companies were subsequently charged in relation to a $45 million bank heist that involved stolen account information. A group supporting Syria's Assad regime hacked the Associated Press' Twitter account, tweeting (falsely) that President Obama had been injured in White House explosions. And a report released by the US government reported that China's People's Liberation Army had carried out cyber attacks on US corporations.

The breadth and high-level nature of cybersecurity incidents that took place just in the past year indicates the

increasing importance of cybersecurity issues. Yet, as P.W. Singer and Allan Friedman point out in*Cybersecurity and Cyberwar: What Everyone Needs to Know*, released January 3rd, policymakers and members of the public alike know little about the nature and seriousness of these threats. The authors were inspired to write the book by this widespread ignorance, particularly by a senior official at the US Department of Defense who declared that "all this cyber stuff" was a pressing concern. As the authors explain, "when he could only describe the problem as 'all this cyber stuff,' he unintentionally convinced us to write this book," (p. 1).

How It All Works

In *Cybersecurity and Cyberwar,* Singer and Friedman attempt to fill this worrisome knowledge gap. The book is divided into three sections: "How it All Works," "Why it Matters," and "What Can We Do?". In the first section of the book the authors briefly explain the basics of the Internet, from IP addresses to email. They also provide a history of the development of the Internet, as well as an overview of its international governance organizations. Their historical discussion points to a number of problems that will become important to preventing and regulating cyberwar and cyber crime. The authors note that the Internet is built around "a dynamic architecture" that promotes both flexibility and resilience (17). This architecture allows the Internet to function "without top-down coordination. But it also shows the importance of the Internet's users and gatekeepers behaving properly, and how certain built-in choke points can create vulnerabilities if they don't" (25). Such vulnerabilities include the Internet's increasingly inextricable connections to critical infrastructure, and the fact that cyber attacks are often routed through a number of different countries and therefore different legal jurisdictions, making sorting out prosecution and the laws involved much more complicated (59). Despite the potentially dry, and certainly basic, subject matter, this section is written in an interesting, engaging, and sometimes humorous way that will be of interest both to beginners and to those with IT expertise who want to have a better understanding of cybersecurity vulnerabilities and threats.

Why It Matters

The second section, Why it Matters, begins with a discussion of terms and definitions. While this might seem mundane or even redundant, it points to several concrete and deeply worrying problems surrounding cybersecurity. As the above mentioned litany of incidents in 2013 indicates, terms like 'cybersecurity' actually comprise a vast spectrum of problems, from denial of service attacks and "hacktivist" activities like Wikileaks' release of classified documents, to malware, financial fraud, stealing patents, or securing critical infrastructure. As the authors point out, lumping these issues together under the catchall heading "cybersecurity" is as absurd as "treating the actions of a prankster with fireworks, a bank robber with a revolver, an insurgent with a roadside bomb, and a state military with a cruise missile as if they were all the same phenomenon simply because their tools all involved the same chemistry of gunpowder" (68). While cybersecurity generally refers to phenomena that involve the same set of tools and techniques, there is a massive variety in the actors and activities involved. The implication is not just that we need more policymakers to understand 'cybersecurity,' but that groups of scholars and policymakers must develop a deeper understanding of the various sub-fields encompassed by this vast field. In other words, we have much further to go in developing a deep understanding of the issues comprised by this term. Such multifaceted terminology is also troubling because, as the authors point out, even when governments want to collaborate on cybersecurity issues, a lack of common vocabulary to discuss and understand them makes such collaboration even more difficult.

Following this, the authors delineate a sort of typology of the different problems encompassed by the term 'cybersecurity'—hacktivism, cybercrime, cyber espionage, cyber terrorism, cyber war, and so forth—as well as the myriad of actors involved—from hacktivists, criminal cartels and other non-state actors, to governments themselves. This section is both helpful and informative, providing real-life examples of threats and actors that animate the discussion and make it more accessible across different levels of expertise. Their short section on the hactivist group Anonymous is particularly interesting (80-84). Your view of Anonymous and its activities may depend on where you stand—are they engaging in a new form of the time-honored practice of civil disobedience, or are they merely petty criminals? Whatever your position, the authors' description of Anonymous' activities, from facing off with a Mexican drug cartel to promoting Internet freedom, helps to illustrate the incredibly complex—and fascinating—problems and potentials that increasing networked connectivity brings. As complex, important, and worrisome as these issues are, however, the authors note that the overarching message is that we need to take the hyperbole often associated with

commentary about cybersecurity with a very large grain of salt. Letting our fears of immanent catastrophe get the better of us will lead to policies that are sub-par, and even destructive in their own right. Yet that should not diminish the dramatically increasing importance of cybersecurity in a globalized world: "how we respond to this world of growing cyberthreats will shape everything from our personal privacy and the future of the Internet to the likelihood of regional crises and even global wars. So we better get it right" (165).

What Can We Do?

The authors address how this could be achieved in the final section of the book, titled What Can We Do? This section is the most interesting portion of the book from a policy perspective, detailing policy frameworks and proposals for building a more secure Internet communications infrastructure. Singer and Friedman's discussion revolves around the concept of "resilience," one that is "both overused and underexplored" (170). The term resilience refers to systems and organizations that "are prepared for attacks and can maintain some functionality and control while under attack" (170). Rather than focusing on building solutions for very specific cybersecurity problems on an ad hoc basis, we should focus on building systems that are resilient, and therefore capable of resisting a variety of different types of threats. In other words, there is not one single 'silver bullet' solution to cybersecurity, but rather different frameworks for thinking that will help develop more robust approaches to achieving cybersecurity in different arenas over time. This must include tracking metrics to guide long-term organizational planning and investment, as well as war game-type exercises, with outsiders attempting to break into cyber defenses in order to discover insecure areas, amongst other techniques and best practices (172).

One framework Singer and Friedman propose is based on the public health system in the US, a non-hierarchical network that is in part centered around the Centers for Disease Control (CDC). Rather than directing activities, the CDC provides research and acts as a coordinating hub for other state, international, and non-state actors in the public health system. According to the authors' proposal, a cyber CDC would address some of the flaws in the system by shifting the focus from quick fix, short-term measures of responding to attacks towards a long-term mode of regional, national, and even international cooperation. Such an organization could also serve as a kind of epistemic community for the cyber world, acting as a sort of neutral middleman in intensely political environments (175). In another framework, the authors suggest thinking about cyber criminals like 16th century pirates: "much like the sea, cyberspace can be thought of as an ecosystem of actors with specific interests and capacities. Responsibility and accountability are not natural market outcomes, but incentives and frameworks can be created either to enable bad behavior or to support the greater public order" (178). Such policy recommendations for future systems of cybersecurity and Internet will be particularly interesting to scholars of IR and global governance, providing a number of compelling possibilities for future research into a field that is relatively understudied and under-theorized.

Takeways

The only readers that may be disappointed with *Cybersecurity and Cyberwar* are those who already have a deeper knowledge of cybersecurity. Because the book is written at a fairly basic level, readers who are already immersed in these issues will not get as much out of it as beginners with little knowledge of cybersecurity issues. However, readers with a higher level of expertise might still glean something useful: IT experts in network security, for example, could skip the first two sections and focus on the policy proposals of the third, while policymakers already familiar with cybersecurity-related policy might gain more from the technical discussions of the first section. The book may also be useful in pedagogical settings, as the authors have provided a number of innovative resources for classroom use, including a dedicated website with discussion questions (and even an accompanying song playlist!) that will make the material more accessible in a classroom setting. The easy-to-read style, sprinkled with colloquial language, humor, and anecdotes, will make the book particularly engaging to students (the authors have also made part of the text available for preview for professors interested in teaching it on CourseSmart).

While scholars and students of IR will find the book to be a helpful reference for learning about and building a deeper understanding of cybersecurity issues, these readers may be left wanting more on the international security implications, and related policy recommendations, of the issues raised by the authors. The second section, Why It

Matters, does include a short but fascinating look at the foreign policy implications of cybersecurity, from cyberterrorism to Internet access as a human right and the ethics of cyber weapons. However, this section may leave readers searching for a more in-depth discussion of foreign policy implications, for example, more concrete policy proposals about what the US Department of Defense should be doing to ramp up protections against inter-state cyber war, or how and whether the State Department should promote Internet freedom as a human right. Similarly, readers versed in IR theory may wonder whether traditional IR theories (eg 'the security dilemma') may be applicable to understanding cybersecurity, or whether IR theorists will have to develop entirely new approaches (a question tackled by Singer in a recent e-IR interview).

Other recent books that provide more detailed discussions of cyberwar and concrete foreign policy proposals include Richard A. Clarke and Robert Knake's *Cyber War: The Next Threat to National Security and What to Do About It* and Joel Brenner's *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* However, it is worth noting that the former has been criticized for its hyperbolic and even fear-mongering tone. One of the refreshing aspects of Singer and Friedman's approach is their even-handed tone and ability to treat pressing security issues without resorting to overstatement or embellishment. Furthermore, rather than provide specific, silver bullet-type policy recommendations, the authors' focus in *Cybersecurity and Cyberwar* is on providing broader avenues for thinking that may help policymakers develop different solutions for the variety of specific empirical problems, rather than generating specific foreign policy proposals. Nevertheless, given the Singer and Friedman's ability to treat this topic in a neutral way and build interesting narratives out of a subject that might otherwise be a bit dry, it would be interesting to hear more from them on what sorts of policies and capabilities governments should be developing on cyber defense and to counter threats like cyberterrorism. Perhaps this will be their next project.

Singer and Friedman's *Cybersecurity and Cyberwar* will have a number of important implications for academic scholars and experts on cybersecurity. Perhaps most importantly, this book will be a significant contribution to building a deeper understanding and a common base of knowledge around cybersecurity issues. This, in turn, may serve as a foundation for enabling policymakers, scholars, and citizens to begin building a crucial dialogue and much-needed conversation around how to approach, understand, and deal with the important policy implications of cybersecurity and cyberwar.

—

Alex Stark *is Features Editor and a Director of e-International Relations. Follow her on Twitter @AlexMStark.*

About the author:

Alex Stark is an Editor-at-large of E-International Relations and a member of E-IR's Editorial board. She is a PhD student in International Relations at Georgetown University. She received her MSc in IR from the London School of Economics and BA from Wellesley College, where she was an Albright Fellow. Follow her on Twitter: @AlexMStark