Going Dark

Summer_2019
Vol_6 No_1

FLETCHER SECURITY REVIEW
OMNIBUS SECURITAS

Going Dark

How Living in a 21st Century World Affects Security and Geopolitics

Summer 2019
Vol. 6 No. 1

About FSR

The Fletcher Security Review (www.fletchersecurity.org) is a print and online journal managed and edited by students at Tufts University's Fletcher School of Law and Diplomacy. At FSR, we aim to build on the school's strong traditions of marrying theory with practice and fostering close interdisciplinary collaboration to act as an incubator for unique perspectives across a broad range of security issues. We hope to provide our contributors a forum for advancing new theses or for innovative approaches to established ones. Because we believe in publishing the work of established and emerging scholars, practitioners, and analysts on topics and from perspectives deserving greater attention, FSR can serve as a distinctive medium in the security field.

Advisory Board

Thank You to Our Sponsors

ISSP
INTERNATIONAL SECURITY STUDIES PROGRAM

Russia and Eurasia Program
U.S.-RUSSIA RELATIONS INITIATIVE

Contact Us

Address Letters to:
Editor in Chief, Fletcher Security Review
The Fletcher School
160 Packard Avenue, Medford, MA 02155

Or by Email:
Editor in Chief, Fletcher Security Review
fletchersecrev@gmail.com

Information for Authors

Please send submissions to fletchersecrev@gmail.com. All submissions should be sent as a Microsoft Word file. Short articles should be 1,500 to 2,000 words and long articles should be 3,000 to 5,500 words.

Referencing

Last Name, First Initial. Middle Initial. (2019). Article Title. *The Fletcher Security Review*, 6(1), Pages.

Credits

Cover Design by Keifer Chiang

Technology touches nearly every part of our daily lives, and *Fletcher Security Review*'s Summer 2019 issue examines the influence technology has on security, whether it be IT or military technology. As editor-in-chief, I encouraged our editors to go beyond the assumptions, and I believe this edition both evaluates and investigates the complexity of technology and security.

This edition was possible thanks to the hard work of many, particularly Annalise Burnett, the managing editor. Annalise assisted in many decisions and willingly took on challenges, in addition to being an excellent editor. As the future editor-in-chief, I am confident she will bring the journal further success. I also must highlight the incredibly talented Keifer Chang, the creative director for *FSR*, for his keen eye and dedication to producing a modern academic journal.

The senior staff members have routinely gone above and beyond in their positions. Thank you to Chloe Logan, Lauren Michaels, Arthur Montandan, Tawni Sasaki, Maia Brown-Jackson, Ryan Rodgers, and Senjuti Mallick for your dedication and leadership. This journal is possible thanks to the hours they spent working with our contributors and encouraging staff editors.

Professor Richard Shultz and the International Security Studies Program have once again generously funded this journal, allowing us to focus on the quality of the articles. The Fletcher Russia and Eurasia program has also provided the critical funding needed to design this journal. Thank you both for your continued support.

I have been honored to work with so many talented people and read so many interesting articles as editor-in-chief. I have aimed to produce a journal that looks critically at the security issues we face today. Thank you to the contributors that have critically evaluated issues facing our world today, and I hope some of your insights and solutions result in a more secure world. I hope you enjoy this summer's edition of *Fletcher Security Review*.

Kacie Yearout
Editor-in-Chief

Military Technologies

National Security

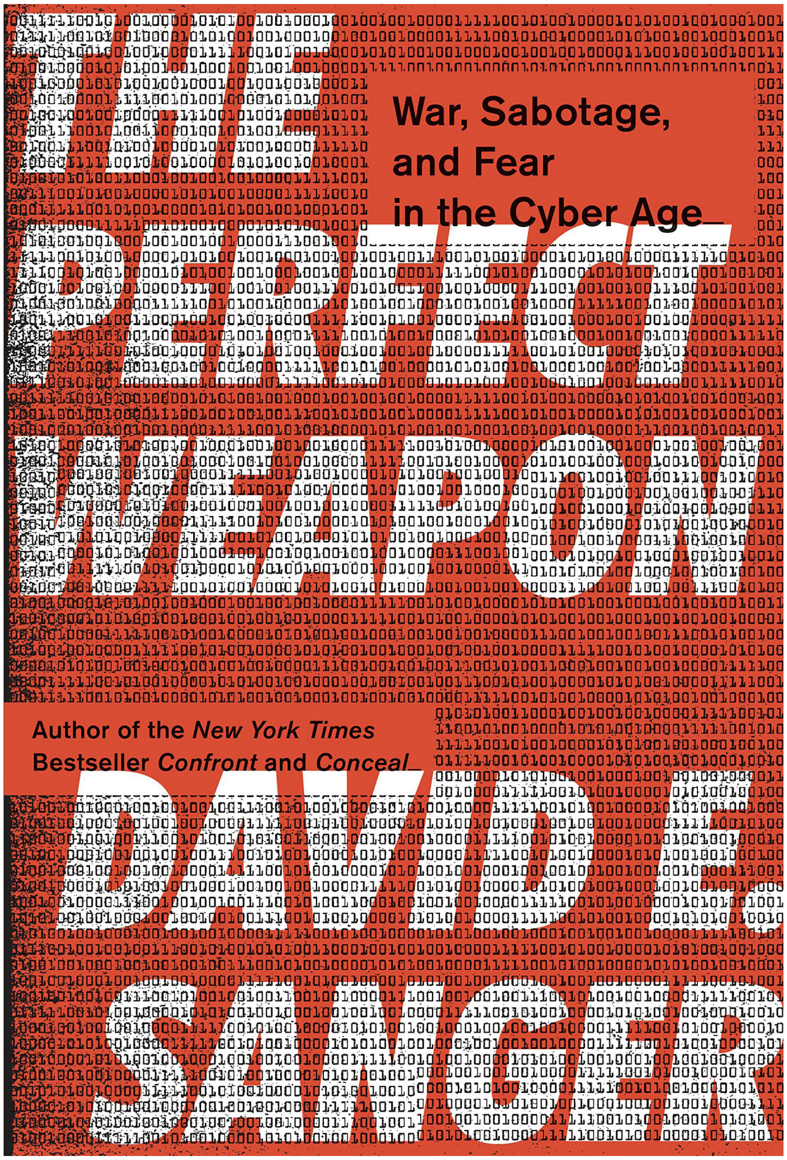
Cyberspace

The Perfect Weapon

War, Sabotage, and Fear in the Cyber Age by David E. Sanger

A Book Review by Travis Frederick

"No modern military can live without cyber capabilities, just as no nation could imagine, after 1918, living without airpower."


War, Sabotage, and Fear in the Cyber Age
Author of the New York Times Bestseller Confront and Conceal

In *The Perfect Weapon,* David Sanger argues that the nature of global power itself is undergoing dramatic changes, brought about by the proliferation of highly advanced cyber capabilities. Today, internet access is nearly ubiquitous, the cost of entry is low, and, particularly in the domain of cyberwarfare, there is one fundamental fact: offensive capabilities have critically outpaced cyber defenses. A weak and impoverished nation like North Korea can hold large swaths of public and private infrastructure in America at risk, steal military OpPlans, and pilfer millions of dollars from foreign banks. A Kremlin reeling from sanctions, low oil prices, and historically low public trust is able to threaten the very foundations of American democracy through targeted social media campaigns and hacking and leaking the emails of a major political party. But while the offensive advantage has given weaker powers greater capacity to pursue their geopolitical objectives, U.S. leadership has found that their response options have not similarly benefitted. America's offensive cyber prowess so exceeds its own defensive capabilities that officials often hesitate to strike back for fear of establishing norms of retaliation against vulnerable infrastructure or inciting unintended escalation. Sanger argues that without an open public debate among government policy makers, military planners, and academics to coordinate a grand strategy, the United States will be forced to accept a world of constant cyberattacks, limited response options, and the greater risk of capitulating to foreign coercion.

Throughout Sanger's numerous interviews in *The Perfect Weapon,* there is an unmistakable tension present in the cyber security views of public officials, intelligence agencies, and private companies. How should they respond to cyberattacks and known defense vulnerabilities? In response to Russian interference in the 2016 U.S. presidential election, some officials advocated retaliation by punishing Russian President Vladimir Putin personally, freezing oligarch money around the world, or by conducting an in-kind hack and leak operation against the Russians. Yet, the most common U.S. response to attacks has been either low-cost symbolic action, or to secure defenses and not respond at all. One Obama-era official noted the reticence to even publicly attribute known attackers because, "Once you say who committed an attack, the next question is, so what are you going to do about it?" Intelligence officials have encouraged this government silence, arguing that by attributing an attack, states reveal both their capacity to monitor their own networks as well as adversary systems. Likewise, they argue that public acknowledgement of one's own offensive cyber capabilities undermines previously secret advantages their forces may have had. Private companies have pushed back against this silence, arguing that the government bears the responsibility to publicly reveal potential attacks or network vulnerabilities once it has found them. Reflecting a lack of confidence in government responses, some tech giants have taken to "active defense"—hacking back. So, how should the United States respond to cyberattacks and known defense vulnerabilities?

The primary argument of *The Perfect* W*eapon* is that despite years of spending billions of dollars on new offensive and defensive cyber capabilities, the United States has failed to create a successful deterrent against cyberattacks. By first acknowledging the folly of going on the offense without a good defense, Sanger advocates for establishing a policy of deterrence by denial. He goes on to provide a set of policy recommendations based on securing U.S. defenses and establishing international norms against cyberattacks. He believes that these two pillars of cyber policy, namely a strong defense and international norms of non-aggression, will most effectively support U.S. national security in the coming decades. This will require a Manhattan Project-like commitment to secure the most critical infrastructure and a set playbook for responding to attacks. This playbook requires that the U.S. enhance its capabilities to attribute attacks and make calling out adversaries the standard response to any and all cyber aggression.

One critique of Sanger's emphasis on deterrence by denial is that it does not introduce costs sufficient to change the calculations of malicious actors. Even with an effort on the scale of the Manhattan Project to shore up U.S. defenses combined with calling out adversaries, it is implausible that the costs of an adversary's failed attempts to penetrate critical networks or public shaming will ever meet the threshold to successfully deter further attacks. During an interview with the author of this review, David Sanger acknowledged the limitations and tradeoffs of a primarily deterrence-by-denial approach. However, he also argued that policy options are constrained by the reflexive secrecy of the national security establishment regarding offensive cyber capabilities, which has effectively undermined any cost the United States may hope to instill in the minds of its adversaries. In order to create any kind of cyber deterrent or engage in any negotiation of limits in cyberspace, the United States is going to have to be willing to acknowledge some of its own capabilities. By pushing back on some of the system's reflexive secrecy, Sanger argues, the United States can acknowledge some of what it can do in order to threaten adversaries, and importantly, what it will not do in order to begin establishing global norms in cyber conduct. Through hardened defense, norms of non-aggression, and progress towards eventual cyber arms control, Sanger hopes that one day a strategic stability will be reached where the world will be able to reap the full benefits of a technological society without being held captive by burgeoning cyber vulnerabilities.

Truly compelling for security scholars and casual readers alike, *The Perfect Weapon* provides a fast-paced, detailed history of cyberattacks. David Sanger adroitly illustrates the central dilemmas of cyber policy and the tensions among its key U.S. actors, all while maintaining a sense of immediate concern for the immense dangers posed by cyber warfare. This book has a breadth and depth that will engage casual readers and urge professors to update their course syllabi with several new chapters.

Travis Frederick

Travis Frederick is a Ph.D. candidate in security studies at Princeton University and a graduate researcher in Princeton's Socio-Cognitive Processes Lab. His research interests include Russian security policy, U.S.-Russia relations, and the psychology of threat perception. He is a Graduate Fellow at the Center for International Security Studies and has previously worked at OSD Policy, U.S. State Department, and GTRI.