Journal of Strategic Security

Volume 12 | Number 3 Article 7

Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat. By John P. Carlin, with Garrett M. Graff. New York: Hatchett Book Group, 2018.

Edwin E. Urie
Retired Department of Defense Intelligence Executive

pp. 179-181

Recommended Citation
Urie, Edwin E.. "Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat. By John P. Carlin, with Garrett M. Graff. New York: Hatchett Book Group, 2018.." *Journal of Strategic Security* 12, no. 3 (2019) : 179-181.
DOI: https://doi.org/10.5038/1944-0472.12.3.1766
Available at: https://scholarcommons.usf.edu/jss/vol12/iss3/7

Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat. By John P. Carlin, with Garrett M. Graff. New York: Hatchett Book Group, 2018.

***Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. By John P. Carlin, with Garrett M. Graff. New York: Hatchett Book Group, 2018. ISBNs 978-1-5417-7383-7 (hardcover), 978-1-5417-7381-3 (ebook). Text, Notes, Sources cited. Index. Pp. 467. $30.00.**

This book can be considered to be an authoritative text, perhaps even an alert, as it describes the current and growing vulnerabilities and attacks on the cyber world. The author, John P. Carlin, is the former Assistant Attorney General for the Department of Justice's National Security Division, who also served as Chief of Staff to then-FBI director Robert Mueller, III, and as National Coordinator of the US Justice Department's Computer Hacking and Intellectual Property (CHIP) program. Currently he is the chair of the Aspen Institute's Cybersecurity and Technology Program, and performs similar functions with the law firm Morrison and Foerster. Garrett M. Graff, with whom Carlin wrote the book, also is with the Aspen Institute's Cybersecurity and Technology Program.

The author's objective is to clearly define and describe what has begun as a Code War, in which the threat online has evolved at the same pace as our reliance on the cyber world for communication, data storage, and international relationships, as well as personal and national financial activities. He recognizes that the global network was not designed with safety and security in mind, and as a result there are those who are relentlessly taking advantage of it. In this respect, the book can be considered a unique recognition of a new, growing national (and personal) vulnerability that has not been otherwise recognized in the public domain.

To place the "war" in perspective, the author notes the rise of terrorism following the 2001 events of 9/11, along with the rise of cyber crime, recognition of the need for counterterrorism actions, and the resulting necessary efforts focused on cyber security. He notes that in 2008, at least ten cyber threats were recognized and early efforts at defensive measures were implemented. This 21st century problem was not limited to detection of cyber attacks, it also raised issues about how to best protect cyber activities, and ultimately the methods and manner in which to prosecute the offenders. The latter issue was complicated by the fact that offenders were not limited to American attackers. Individuals and government elements of a variety of foreign countries were actively conducting these

attacks, most notably those of China. Chinese attacks, in particular, were resulting in serious impact on the U.S. economy.

Further complicating this rather dire situation was the recognition in that same period that our own U.S. government agencies were not effectively sharing information, both in terms of inter-agency and intra-agency, especially among the seventeen or so elements of the U.S. Intelligence Community. Of course, efforts to appropriately share information also placed this information in more vulnerable target areas. Several of the Intelligence Community Agencies, in recognition of both parts of this problem, were in the process of improving the sharing of intelligence products, so some efforts also were made to recognize the cyber threat and take measures to reduce it.

Another cyber threat recognized in the first decade of the 21st century was that of the threat to political activities. Evidence was found that Chinese hackers in 2008 were conducting an espionage operation by successfully penetrating the computer network of the Democratic Party and gaining information regarding presidential campaign activities and plans. Originally this problem was thought to be an ordinary computer virus, however, it was found to be malware that was enabling the Chinese to access policy documents and campaign planning information. The FBI had already been providing defensive briefings to political entities in the assumption that they could be targeted by foreign intelligence agencies, but such cyber attacks during a presidential campaign were not expected. Soon after this recognition the FBI learned that similar cyber attacks were also successfully being conducted against Republican Party networks. The author clearly states the outcome of these cyber attacks: “Ultimately, the 2008 presidential campaign hack was another missed alarm bell, a missed chance to understand the importance of cybersecurity on the geopolitical agenda” (69).

Recognition of this cyber security problem finally has resulted in changes in Federal regulations to enable easier access and recognition of probable hackers. New government authorities have been established to this effect, recognizing that the cyber threat is a national security threat, and it must be identified and both defensive and retaliatory actions must be taken.

https://scholarcommons.usf.edu/jss/vol12/iss3/7
DOI: https://doi.org/10.5038/1944-0472.12.3.1766

What might be the most significant virtue of this book is the value of the information in intelligence, counterterrorism, and protection, as well as important usefulness to individuals regarding their personal financial data and other communications. With the continuing rise in the use of social networks via computers, smart phones, and other means, recognition of the potential problem is highly noteworthy. In this respect, one need not be a computer expert in order to read and understand the current situation and objectives of this book and the nature of the cyber threat. The book is certainly worth buying, studying, and recognizing the threat, then taking the protective actions provided.

Edwin E. Urie, Henley-Putnam University Professor, Retired
Department of Defense Intelligence Executive