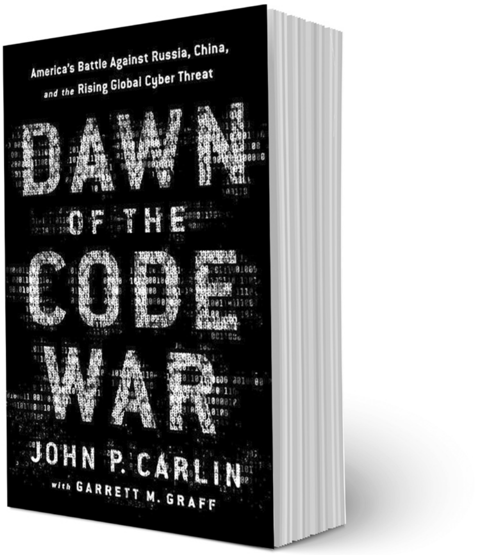
Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat

by John P. Carlin

Reviewed by
Philip C. Shackelford


America's Battle Against Russia, China, and the Rising Global Cyber Threat
DAWN OF THE CODE WAR
JOHN P. CARLIN
with GARRETT M. GRAFF

EXECUTIVE SUMMARY

"Winning the Code War first requires recognizing that the war has already begun."

With this final sentence in the Epilogue, John Carlin, former Assistant Attorney General for National Security, summarizes the central thrust of his book—telling the story of how "criminals, terrorists, and spies made themselves at home on a global network that was never designed with safety and security in mind" and detailing the ways in which the United States government, prosecutors, the FBI, and our allies around the world have spent twenty-five years "playing catch-up." *Dawn of the Code War* is part memoir, as Carlin himself was intimately involved with many of the struggles he describes; part history that chronicles high points in the development of cyber threats since the beginning of the Internet; and part warning as Carline reminds us that we have "built our modern society on top of fragile technology, with far too little thought as to the creativity of our adversaries." Carlin does not rest his argument solely on the context of his direct involvement in the "Code War," but supports his narrative with a robust combination of public media sources and government and corporate documents and press releases. Carlin covers technical details in a manner that allows the reader to have a broad understanding of developments without bogging the text down in unnecessary minutiae. This result is a novice-friendly approach that promotes the "big picture" perspective Carlin seems to favor. Carlin succeeds in "demystifying" the realm of cyber war, raising awareness of the threat landscape, and highlighting thought-provoking questions about our dependence on the Internet and approach to cyber threats.

Philip Shackelford is the Library Director at South Arkansas Community College in El Dorado, Arkansas. He currently serves as Awards Chair for the Arkansas Library Association as well as Secretary of ARKLink, the Arkansas Academic Libraries Consortium. His historical research focuses on the Cold War history of the U.S. Air Force, the Air Force Security Service, and the history of intelligence and national security during the early Cold War. His recent article "Fighting for Air: The Struggle for Air Force COMINT, 1945-1952" was published in the *U.S. Military History Review*, and Philip continues to write, research, review, and publish in this area. Philip holds a Master's degree in History and a Master's degree in Library and Information Science, both from Kent State University in Kent, Ohio.

REVIEW

A central thread throughout *Dawn of the Code War* relates to cybercrime and law enforcement, and the difficulty of figuring out how to "impose the laws and rules of the physical world" onto a virtual place "you can't see but you know is there." One issue is determining the financial damage to companies, governments, and individuals because of cybercrime. Another is understanding how to bring existing laws and legal standards to bear on a category of criminal activity that Carlin believes is still in its infancy and that, particularly early on, did not have direct, applicable legal parallels. Indeed, some of the earliest examples of cybercrime were legally defined as making obscene or harassing telephone calls or breaking and entering. The U.S. government did not yet possess an applicable framework for prosecuting cybercrime. Such issues conflicted with the popular belief that the Internet was a free and open tool for education, discovery, and expression. At the time, few could imagine the extent to which the Internet would become integrated with so many aspects of our daily lives. This dependence on the Internet amplifies the risk at hand—Carlin uses the analogy that we are "living in an online house of straw, yet even as the wolf approaches the door, not only are we not seeking shelter in a stronger house, we're continuing to cram ever more stuff into our straw house."

Cybercrime did not remain limited to innocent, prankster-like activity for long, as the Internet soon became a hub for criminality and malicious attacks. Cybercrime and cyberwar continue to defy traditional definition. They are a "complicated, multidimensional, international" tension that requires resources and attention from both government and private sectors. The Code War does not involve a single set of opposing actors or ideologies but is characterized by myriad and anonymous adversaries and vulnerabilities.

Carlin identifies three distinct “epochs” of evolving cyberthreats and believes that we are moving into a fourth. First, he emphasizes China and its practice of engaging in economic espionage, stealing government and corporate secrets. His second “epoch” begins in the late 2000s, when Iran began conducting destructive digital attacks, including an attempt to assassinate the Saudi ambassador in a Washington, D.C. restaurant, followed by digital attacks on the Wall Street financial sector and a Las Vegas casino owner. Third, North Korea fused digital attacks with social media awareness to amplify the impact of their attack. Finally, Carlin believes that we are seeing the emergence of a fourth “epoch” in which bad actors—both nation-states and non-state actors—combine cyberattacks with real-world “kinetic” attacks. Examples of this include targeting power grids, hospitals, and the Internet of Things.

Not only has the rise of the Internet exposed modern society to “complex and unprecedented” threats, but Carlin points out that it has fundamentally blurred our understanding of the world as well, in six different ways. Specifically, the Internet has blurred the lines between peace and war, between public and private, the nation-state vs. the individual, physical vs. virtual, distinctions between borders, and obscured our understanding of what is “secret” and what is “critical infrastructure.” These obfuscations have profound implications as government officials and lawmakers struggle with an inadequate vocabulary for describing and framing attacks. What constitutes an act of war? What is “critical infrastructure?” What does an appropriate and proportional response look like?

Hence comes Carlin’s word of warning—his position that our approach as a nation and society remains “inadequate.” Our progress remains “too slow” online. We need to think faster, smarter, and take full advantage of basic security practices that would protect from many day-to-day threats. More broadly, Carlin emphasizes that little will change unless the fundamental designs and standards of the Internet—elements that are inherently insecure and have been since the beginning—are sufficiently updated with a focus on security by design.

CONCLUSION

Carlin successfully highlights the development of cyber threats since the rise of the Internet and provides valuable, thought-provoking insight into cybersecurity. He presents useful questions and suggestions to prepare for the road ahead. In his conclusion Carlin is perhaps overly kind in his assessment of American values as they pertain to the cyber realm—China is not the only modern society making “Orwellian advancements” in facial recognition technology and “ubiquitous” video surveillance. Nevertheless, *Dawn of the Code War* is a sweeping yet intimate picture of the current cyber threat landscape that correctly emphasizes the priority of cyber defense.

Title: *Dawn of the Code War:*
America’s Battle Against Russia, China, and the Rising Global Cyber Threat

Author: John P. Carlin with Garrett M. Graff

Publisher: Public Affairs (October 2018)

Hardback: 468 pages

Language: English

ISBN: 978-1-5417-7383-7

Price: $30.00