the
LAWFARE
BOOK REVIEW

Out of the Blue and into the Black?

JOHN SIPHER

Review of Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (Simon & Shuster 2016)

An article in the New York Times several weeks ago reported on the U.S. "cyber war" against ISIS. One of the quoted sources in the article even used the term "cyber bombs" to describe activities against ISIS. While the article barely raised any public reaction, it was nonetheless notable in that the U.S. government rarely discusses publicly its national security efforts in the cyber realm. And for good reason. We don't want our adversaries to be aware that they are being "attacked." Nor is it clear that the U.S. has adequately come to terms with the ramifications of our offensive cyber prowess, not to mention that we have yet to deal with the massive vulnerabilities of our infrastructure to hacking, cyber espionage, cyber terrorism and cyber war.

What do these "cyber" terms actually mean? Are efforts to hack and damage foreign computer networks acts of war? Does the Congress need to declare war before we can utilize these tools? Have we thought through our own vulnerabilities if adversaries respond in kind... or are we paralyzed by the prospect of retaliation and unscripted escalation? Are we comfortable with the NSA and military dominating this realm? What role should the government play in helping to protect the networks of private U.S. companies?

Fred Kaplan's new book, *Dark Territory: The Secret History of Cyber War*, is the best available history of the U.S. government's secret use of both cyber spying, and efforts to use its computer prowess for more aggressive attacks. While the book does not tackle the systemic issues head-on, it provides a readable background and overview to help frame a public, policy and national security debate that can't be elided forever – or even for very much longer.

Kaplan is a long-time, highly regarded journalist and author on national security issues who, among many other distinctions, won the Pulitzer prize for his series "War and Peace in the Nuclear Age." He has also written several general-reader books on nuclear and military policy, including, for example, the highly regarded *The Insurgents*, on General David Petraeus' efforts to force the U.S. Army to adopt counterinsurgency precepts in Iraq. He is well placed in policy expertise and journalistic sources to undertake an overview of national security cyber issues for a broad audience.

Dark Territory is thus unsurprisingly written in a general reader-friendly style.

Its substance contains a number of fascinating, little-known stories about the National Security Agency and other secret units of the U.S. military and intelligence community. However, since Kaplan is writing about one of the most secret aspects of U.S. intelligence and military policy, these stories sometimes leave the reader wanting additional detail. This was a complaint levied by the reviewer for the New York Times, for example, suggesting that too much of the book merely describes the results of various "blue ribbon" panels trying to wrestle with how to energize U.S. institutions, public and private, to face up to the vulnerability of their networks. Given its subject, however, it is not surprising that Kaplan couldn't provide more specifics on covert operations. I'm not exactly sure what the New York Times could have expected from Kaplan. As a former intelligence officer, I found myself often uncomfortable that he was revealing as many details as he did.

Nonetheless, *Dark Territory* is an especially valuable addition to the debate on a number of fronts. You can't read Kaplan's book without realizing that the U.S. is more vulnerable than most any other country on earth to cyber attacks. No society is more dependent on its Internet infrastructure than the U.S. Moreover, the numerous fascinating stories of U.S. success in penetrating and disabling foreign computer networks only serve to highlight how easy it would be for them to attack us. As Kaplan says, "If America wanted to wage a cyber war, it would do so from a glass house. Anything we can do, they can do to us."

Indeed, since the time that President Ronald Reagan asked for an assessment of U.S. information security after watching the popular Matthew Broderick movie "War Games," one blue ribbon panel after another has been warning about our vulnerability to hackers and cyber-sleuths. And there has been amazing (and equally dismaying) consistency in their findings. The string of reports over 35 years read almost as if they are slightly edited facsimiles of their predecessors. For all that, however, the breathlessness of these warnings has not really translated into action. Director of National Intelligence James Clapper, for example, has warned that the cyber threat is the number one challenge facing the U.S. – and says it is a larger threat than terrorism. At least one of his predecessors (Mike McConnell) routinely warns of a looming cyber Pearl Harbor or cyber 9/11.

Yet if this is such a looming danger, why have these consistent warnings not translated into the level of action necessary to face the threat? Reading Kaplan's history, I see two basic reasons. First, defending computer systems to the extent necessary is expensive, and the corresponding gains are not clearly visible. More importantly perhaps, serious effort to strengthen U.S. cyber defenses (in both the public and private sectors) is far more boring than investing in sexy offensive cyber tools. Indeed, my guess is that most people who buy Kaplan's book will do so in order to gain a glimpse into the stories of our cyber spies over the years – code breaking, cyber espionage, snooping and even damaging of foreign infrastructure through cyber attacks.

In this regard, *Dark Territory* illuminates the long tension, and notable imbalance, between offensive and defensive cyber capabilities. These tensions were evident from the earliest years of the NSA and are certainly no less evident today. From the very beginning, there was always more funding for and attention to SIGINT

(offense) than INFOSEC (defense). The book's stories of cleverly damaging the Iranian nuclear program from afar are far more engaging than stories of adding layers of protection to unclassified networks in order to thwart attacks.

Second, a barrier to dealing with the threat is its sheer size and scope, coupled with the fact that no one government department, agency, or individual is in charge. The issues at play are huge and thorny. Should we use our impressive cyber capabilities for espionage purposes (to discreetly steal information) – or instead to damage and destroy our enemies' infrastructure ("cyber bombs")? In the debate at the dawn of the nuclear age, the then-recent Pearl Harbor attack galvanized thinking about the ramifications of a nuclear first strike, and focused attention on how to prevent and deter future strikes. A system of deterrence in the cyber realm is far less clear, however. What does deterrence look like in the cyber realm – especially when it might not be clear who attacked you? At what point does cyber war become a real war? Can we respond with bombs to a computer attack and if so under what circumstances?

While the government has found it hard to balance its offensive capabilities with its defensive responsibilities, the private sector has also been complicit in the failure to address the problem in a serious way. Companies often don't report attacks, nor do they wish to admit the scale of their vulnerability for fear that it will impact public trust and ultimately the bottom line. While there is some interest in the banking sphere and Silicon Valley, most people and private firms are just not motivated to take real action. To add insult to injury, the only U.S. institution with the expertise and capability to address these issues is the NSA. And yet, since the Edward Snowden revelations, many private companies with an international footprint do not want to be associated in any way with the U.S. Intelligence Community.

Recent news stories of Iranian hacking attacks against Las Vegas Sands CEO Sheldon Adelson and North Korean attacks against Sony Pictures have begun to raise the private sector issues in the public consciousness. What has not filtered into the public consciousness, however, is just how simple these attacks are to carry out. Breaking into computer systems and doing damage can be done by lone hackers. U.S. government "Red Cell" teams routinely have success breaking into heavily defended U.S. military and diplomatic networks. What's interesting about these attacks by the Iranians and North Koreans is that they took highly public actions in order to send a message. They could easily have done much more damage if they wished. Nonetheless, short of a more visible breach, the mass intellectual-property theft through cybercrime is already costing U.S. industry hundreds of billions of dollars.

Dark Territory is packed with stories about successful U.S. penetration and manipulation of foreign computer networks. The deployment of the Stuxnet virus to damage Iranian nuclear centrifuges was perhaps the most artful from a technical standpoint. The Stuxnet story has been told in many books, of course, but *Dark Territory* ranges across many areas of national security beyond Stuxnet. Kaplan provides, for example, an alternative narrative to the eventual 2006-2007 turnaround in Iraq. While much public credit for the success against Al Qa'ida in Iraq is attributed to President Bush's surge and the efforts of General McChrystal's special forces, Kaplan says,

those in the know attribute the turnaround to the deployment of NSA officers and tools to the front line which helped to pinpoint the location of terrorist cells.

Dark Territory also offers background on the domestic surveillance program that created so much controversy in the wake of Edward Snowden's defection. The technological shift in the U.S. from analog to digital communication in the late 1990s and 2000s allowed for a radical advance in the capability of the NSA and others to collect, store and process data. No longer did the NSA need to listen to and translate individual phone calls. Instead, it could collect massive amounts of data and run algorithms in search of exploitable patterns. This cutting edge use of Big Data was a much more fruitful means to find individual spies and terrorists. And yet – whereas the NSA was doing exactly what it was supposed to do, and exactly what Congress authorized – neither the NSA nor Congress understood that the public might see "bulk collection" in a wholly different light.

Beyond providing insight into today's cyber policy debates, *Dark Territory* also provides a highly readable history of the key players and institutions involved in the development of U.S. cyber policy. Many of the names of those who crafted policy behind the scenes are familiar, from Bobby Ray Inman to William Perry, General Michael Hayden, Mike McConnell, Keith Alexander, Richard Clarke and Robert Gates. The combination of important public policy and national security debates with key players and personalities in the U.S. national security communities make *Dark Territory* an engaging and useful read.

John Sipher is a client services Director at CrossLead, a leadership software service; he retired as a 28-year veteran of the CIA's Clandestine Service.

Cite as John Sipher, *Out of the Blue and into the Black*, Lawfare (June 8, 2016), at https://www.lawfareblog.com/out-blue-and-black.