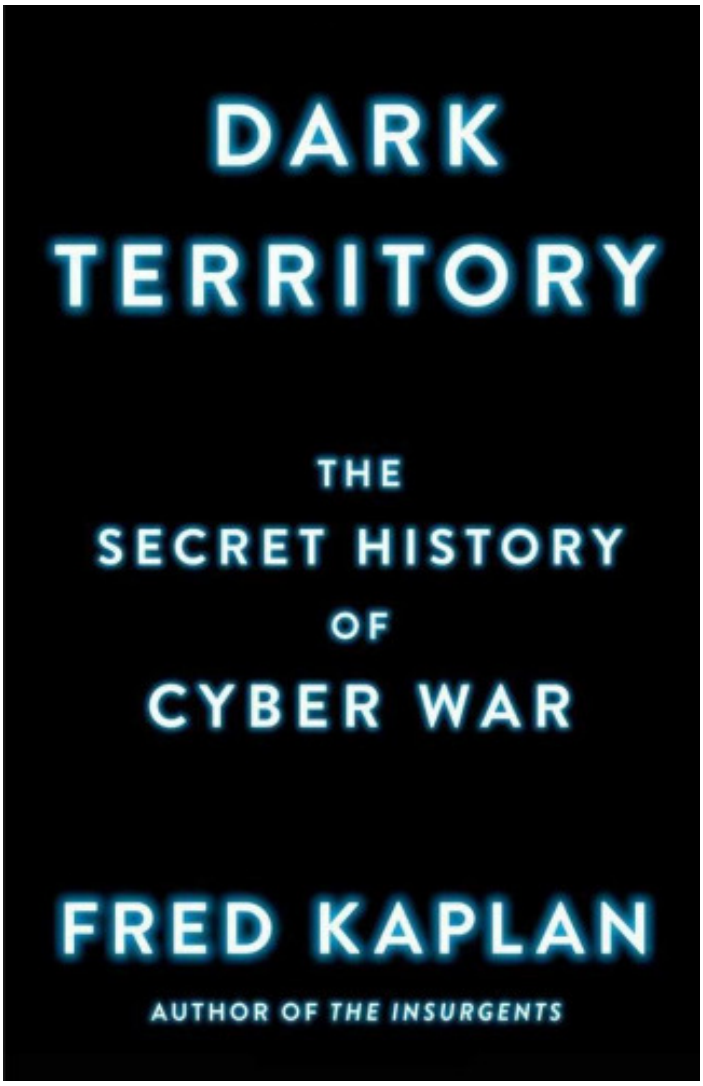
BOWLING GREEN DAILY NEWS

‘Dark Territory’ could raise anxiety

Posted: Sunday, May 8, 2016

“Dark Territory: The Secret History of Cyber War” by Fred Kaplan. New York: Simon & Schuster, 2016, 352 pages, $28.00.



“During Barack Obama’s presidency, cyber warfare took off, emerging as one of the few sectors of the defense budget that soared while others stayed stagnant or declined,” Fred Kaplan explains hear the beginning of “Dark Territory: The Secret History of Cyber War,” his terrifying new account detailing information technology’s ongoing transformation of the nature of international conflict.

“In 2009, Obama’s first secretary of defense, Robert Gates, a holdover from the Bush years, created a dedicated Cyber Command. In its first three years, the command’s annual budget tripled, from $2.7 billion to $7 billion (plus another $7 billion for cyber activities in the military services, all told), while the ranks of its cyberattack teams swelled from 900 personnel to 4,000, with 14,000 foreseen by the end of the decade.”

“The cyber field swelled,” Kaplan continues. “By the midpoint of Obama’s presidency, more than 20 nations had formed cyber warfare units in their militaries. Each day brought new reports of cyber attacks, mounted by China, Russia, Iran, Syria, North Korea and others, against the computer networks of not just the Pentagon and defense contractors but also banks, retailers, factories, electric power grids, waterworks – everything connected to a computer network, and, by the early 21st century, that included nearly everything. And, though much less publicized, the United States and a few other Western powers were mounting cyber attacks on other nations’ computer networks, too.”

Back in the early 1980s, Willis Ware, one of the founders of the increasingly important business of computer security, warned that the only truly secure machine is one that no one uses. “Dark Territory” is a testament to the definitive accuracy of Ware’s prophetic declaration. As I was

reading Kaplan's captivating prose, I was reminded of the current tug-of-war taking place between Apple and the Justice Department. One of the basic premises on which the book is based is the notion that once a technological capability has been unleashed, there is no guarantee it will not be used for far more nefarious purposes than those precipitating its original development. And as Kaplan makes abundantly clear, whatever we do that provides us with a temporary advantage on the cyber front can always be replicated by others – and often in a fraction of the time it took us to do it.

"Dark Territory" is extensively researched with 32 pages of references at the conclusion of the 15 chapters that make up the main text. Much of the volume is based on interviews with more than 100 key players in the story Kaplan is telling, including six National Security Agency directors. The literary style is fluid and authoritative; you definitely get the impression this is an author who knows his subject matter intimately.

As much as I was intrigued by the implications of his thesis for our present and future well-being, however, it was the historical dimension of the narrative that really piqued my interest and kept me up way past my normal bedtime on a couple of occasions.

"As far back as Roman times, armies intercepted enemy communications," Kaplan writes. "In the American Civil War, Union and Confederate generals used the new telegraphy machines to send false orders to the enemy. During World War II, British and American cryptographers broke German and Japanese codes, a crucial ingredient (kept secret for many years after) in the Allied victory. In the first few decades of the Cold War, American and Russian spies routinely intercepted each other's radio signals, microwave transmissions and telephone calls, not just to gather intelligence about intentions and capabilities but, still more, to gain an advantage in the titanic war to come."

Moreover, I was awestruck by the story of how Ronald Reagan's viewing of "War Games," the 1983 movie starring Mathew Broderick about a teenage hacker who inadvertently almost brings about the end of the world, led to presidential directive NSDD-145, which called for the creation of a National Telecommunications and Information Systems Security Committee. If you think today's political squabbling is bad, wait until you read about the hijinks that ensued once Congress got a hold of the mandate. It turns out debates and power struggles related to the appropriate role of the NSA are not a recent phenomenon.

Even though the book deals primarily with how nations – and terrorist organizations – use progressively more sophisticated technologies and strategies to spy on one another, the repercussions for our personal dependence on the internet, which has been growing exponentially for around three decades, are clear and not very reassuring.

"It's a cat-and-mouse game that has a lot of cats and mice running around, of all stripes, and into holes of various provenance," Kaplan said in a recent interview posted on the Council on Foreign Relations website. "If somebody really wants to come after you; if there's something that you have that he wants, and he really knows what he's doing, they're going to get in."

If you found "Terrorism in Cyberspace" by Gabriel Weimann (reviewed Jan. 10) frightening, "Dark Territory" will take your anxiety to the next level. Fair warning: Once you start reading this one, you probably won't be able to put it down. Recommended highly.

Reviewed by Aaron W. Hughey, Department of Counseling and Student Affairs, Western Kentucky University.