Journal of Strategic Security

Volume 9
Number 2 *Summer 2016*

Article 7

# Dark Territory: The Secret History of Cyber War. By Fred Kaplan. New York: Simon & Schuster, 2016.

Edward M. Roche, Ph.D, J.D.,

*Affiliate Researcher, Columbia Institute for Tele-Information, Columbia Business School, Columbia University in the City of New York*


pp. 122-124

***Dark Territory: The Secret History of Cyber War*. By Fred Kaplan. New York: Simon & Schuster, 2016. ISBN 978-1-4767-6325-5. Notes. Sources cited. Index. Pp. ix, 338. $28.00.**

*Dark Territory* is a history of cyber war covering 1967 to the present. The author has a Ph.D. in political science from MIT and writes the "War Stories" column for *Slate*. He won the Pulitzer Prize when working as a reporter for the *Boston Globe*. His other books include *The Insurgents: David Petraeus and the Plot to Change the American Way of War,* published in 2014.

In 1980, the Morris worm took out six *thousand* UNIX computers in the military. In 1983, President Reagan watched *WarGames*, and asked if it was realistic. He was told it was. The result in 1984 was the "National Policy on Telecommunications and Automated Information Systems Security" NSDD-145. This put the National Security Agency (NSA) in charge of ensuring security of communications. Thought also was being given to "counter-C2 warfare," the use of technology to intercept, disrupt and even sever enemy communications. In 1990, National Security Directive 42 authorized tests of a no-notice interoperability exercise (NIEX) targeting the US military. Named Eligible Receiver 97, the entire U.S. defense establishment was penetrated in less than four days, and in the process, traces of French hacking of DOD were discovered. The Solar Sunrise hack originated in the United Arab Emirates and penetrated more than a dozen military bases. Some of the most sensitive systems were hacked by teenagers in San Francisco. The Moonlight Maze hack originated in the Russian Academy of Sciences and took 5.5 gigabytes of data, about three million pages. The People's Republic of China took more than 9.5 terabytes of data from Lockheed on the new joint strike fighter. The Chinese now have a remarkably similar aircraft.

Richard Clarke started to investigate, and even visited hacker groups like L0pht in Cambridge, Massachusetts. These unkempt hackers even briefed President Clinton personally, who then signed Presidential Decision Directive, PDD-63 on Critical Infrastructure Protection. Clarke tried in vain to set up government-private sector cooperation to combat cyber threats, but the private sector refused to cooperate. This problem even today is still with us.

Operation Desert Storm was the first known use of cyber in warfare. The first act was bombing the network switches servicing the fiber-optic cable Saddam Hussein had run from Baghdad through Basra to Kuwait City. Saddam was forced to switch to microwave, all of which was intercepted. A conflict developed between General Schwarzkopf and intelligence. Intel wanted to

disable facilities, the general wanted to bomb, and bomb he did. Lawyers wondered if information warfare which works without dropping bombs was subject to the Law of Armed Conflict, an issue still debated.

During the Bosnia-Herzegovina war, offensive cyber attacks paralyzed the Serbian government. Phones were tapped, GPS transmitters placed in cars, cameras placed in objects resembling rocks, TV transmitters were interrupted, the Serbian paramilitary forces were turned against their own military, recordings of Milosevic cursing were posted on the Internet.

The world of intelligence was changing. By 1993, Rear Admiral Mike McConnell was finding that NSA antennas were going dark. Adversaries were going digital, but NSA was not prepared. By 1995, Jamie Gorelick was warning President Clinton that critical infrastructure was threatened by cyber. As the United States developed methods of cyber penetration of foreign networks, it discovered the United States was even more vulnerable. Everything we can do to them, they can do to us, and more. By 1996, the U.S. Department of Defense (DOD) was getting 250,000 hacks per year, and two-thirds were successful. There was warning of a "cyber equivalent of Pearl Harbor" (48). The United States did not wish to complain, because it was doing the same to others. Offensive cyber plans had been developed for the 1994 invasion of Haiti; by paralyzing the phone system, all air-defense would be disabled.

In 1999, Mike Hayden, at NSA, started a new mission for cyber warfare staffed by the new Information Operations Technology Center (IOTC). He discovered that in spite of its vast budget, NSA was spending less than two million dollars per year on Internet penetration. There were other problems. In January, 2000, the entire NSA crashed and was down for three days. Hayden's Trailblazer project looked to outside contractors, burned up more than $1.2 billion, and was a disaster. CIA "black-bag" operatives were being used to plant eavesdropping equipment. Hayden created the Office of Tailored Access Operations (TAO). Laptop microphones could be monitored. Files could be taken via radio signals even if a PC was not connected to the Internet. Cell phones were tracked. Malware could be introduced wirelessly from miles away. Computer video signals could be intercepted to see what was on the screen. Every possible software and system was intensively tested for vulnerabilities. Then 9/11 happened. The 2003 *National Strategy to Secure Cyberspace,* signed by the president, still faced private sector opposition.



http://scholarcommons.usf.edu/jss/vol9/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.9.2.1532

More cyber operations took place in Iraq. Insurgents were sent false messages dispatching them to places where U.S. Special Forces would kill them. Chips in cell phones could be tapped. Phones could be used for tracking, *even when they were turned off*. Keith Alexander, now at NSA, and his West Point classmate General Stanley McChrystal put in place the Real Time Regional Gateway (RTRG) system which slashed the intelligence cycle, from collection to action, from sixteen hours to one minute, a truly remarkable accomplishment.

In 2007, Israel bombed an unfinished nuclear reactor in Syria, shielded by a U.S. Air Force developed program than tricked Syrian radar. A few months later, the nation of Estonia was shut down by a Russian cyber attack. In 2008, fifty-four Georgian government websites were disabled as Russian tanks rolled across its border. The Aurora Generator Test showed an electricity generator blown up by cyber action. The Natanz reactor in Iran was blown up by Stuxnet, and Iran wiped out tens of thousands of hard drives in Saudi Arabia. NSA's Cyber Command was created during the Obama administration in 2009 by Robert Gates. More than twenty nations have formed cyber units in their militaries.

*Dark Territory* continues its coverage up until late 2015, but I'll leave this truly exciting account for the reader and not spoil the fun. *Dark Territory* does not present an argument one way or the other. It takes no position. But it is a thorough assessment of the political history of the hacking problem as it was faced by the national security establishment of the United States.

*Dark Territory* should be read by anyone interested in national security, and *studied* by anyone interested in SIGINT or the National Security Agency, Cyber Command, and the development of offensive cyber weapons. It offers a carefully balanced presentation of how technology and public policy intertwine, and the defense dilemma posed because unlike with nuclear weapons, in cyber there is no deterrence. But make no mistake about one major takeaway: It is simply not possible to defend against sophisticated cyber attacks, and the United States is more vulnerable than any other nation to this threat.

*Reviewed by Edward M. Roche, Ph.D, J.D., Affiliate Researcher, Columbia Institute for Tele-Information, Columbia Business School, Columbia University in the City of New York*