Cybernar - A Brief Overview

W M 1584

Here is a research report I have prepared, to provide you with a brief introduction to a special threat which will inevitably occur in America—and elsewhere. Indeed, on a small scale, it is already occurring. —*vf*

"**With very little investment, and cloaked in a veil of anonymity, our adversaries will inevitably attempt to harm our national interests. Cyberspace will become a main front in both irregular and traditional conflicts.** Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. **Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains.** In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Indeed, **adversaries have already taken advantage of computer networks and the power of information technology not only to plan and execute savage acts of terrorism**, but also to influence directly the perceptions and will of the U.S. Government and the American population."—*"The Joint Operating Environment." Report released Feb. 18, 2010, pp. 34-36.*

Cyberwarfare (sometimes referred to as "cyberwar" and "cyber warfare") is the use of computers and the internet to conduct warfare in, what the U.S. Department of Defense calls, cyberspace.

One U.S. agency, the *Joint Forces Command*, describes some of its attributes: Lt. Gen. Keith B. Alexander, first head of the recently formed *Cyber Command*, told the *Senate Armed Services Committee* that **computer network warfare is evolving so rapidly that there is a "mismatch between our technical capabilities to conduct operations and the governing laws and policies."**

Cyber Command is the newest global combatant headquarters, whose sole mission is cyberspace, outside the traditional battlefields of land, sea, air and space. It will attempt to find and, when necessary, neutralize cyber attacks and to defend military computer networks *(New York Times, April 14, 2010).*

Alexander sketched out the broad battlefield envisioned for the computer warfare command, listing the kind of targets that his new headquarters could be ordered to attack—including "traditional battlefield prizes, command-and-control systems at military headquarters, air defense networks, and weapon systems that require computers to operate."—*Ibid.*

Cyberspace technology is emerging as an "instrument of power" in societies, and is becoming more available to a country's opponents who may use it to attack, degrade, and disrupt communications and the flow of information. With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad. Furthermore, **"the globe-spanning range of cyberspace and its disregard for national borders will challenge legal systems and complicate a nation's ability to deter threats and respond to contingencies"** (*"The Joint Operating Environment." Report released Feb. 18, 2010, pp. 34-36).*

Governments, their militaries, law enforcement, the private sector, and criminals (individuals or groups) around the world are taking the initiative to train their people in the field of cyber warfare. The necessary skills that a cyber warrior possesses will vary in magnitude; however, **the key skills include: information security, hacking, espionage, and computer forensics.**

Cyber warfare terrain includes **all aspects of the internet, from the backbones of the web to the Internet Service Providers, to the various types of data communication mediums and network equipment.** The terrain does not end in a field, mountain range, or a coastline; rather, the cyber warfare terrain encompasses the cities, communities, and the world in which we live. **The 21st century battlefield has many components, including the internet and all things that connect from a computer to the internet.** This would include: web servers, enterprise information systems, client server systems, communication links, network equipment, and the desktops and laptops in businesses and homes. **The terrain also encompasses information systems like the electrical grids, telecommunication systems, and various corporate and military robotics systems.**

One cyber warfare scenario, ***Cyber ShockWave*, which was war-gamed on the cabinet level by former administration officials**, raised issues ranging from the National Guard to the power grid to the limits of statutory authority *("Cyber ShockWave Shows U.S. Unprepared for Cyber Threats," Los Angeles Times, February 17, 2010).*

The "fog of war" in cyber warfare is **what constitutes an act of war; or even ascertaining who the enemy is could be highly problematic** *(The Tech Herald, Spring 2010).*

Strategists must be aware that part of every po-

DATE OF PUBLICATION: JANUARY 2011

litical and military conflict will take place on the internet, says Kenneth Geers.

There are several methods of attack in cyberwarfare. The following list is ranked in order of mildest to most severe:

Cyber espionage: Cyber espionage is the act or practice of **obtaining secrets (sensitive, proprietary, or classified information) from individuals**, competitors, rivals, groups, governments, and enemies for military, political, or economic advantage by using illegal exploitation methods on internet, networks, software, and/or computers.

Web vandalism: Attacks that **deface web pages or denial-of-service** attacks. This is normally swiftly combated and of little harm.

Propaganda: Political messages can be spread to anyone with access to the internet or any device that receives digital transmissions from the internet to cell phones.

Gathering data: **Classified information that is not handled securely can be intercepted and even modified**, making espionage possible from the other side of the world.

Distributed Denial-of-Service Attacks (DoS): **Large numbers of computers controlled by one person launch attack against systems.** The overwhelming number of attempted accesses crowds out legitimate users who need to access the service.

Equipment disruption: **Military activities that use computers and satellites for coordination are at risk** from this type of attack. Orders and communications can be intercepted or replaced, putting soldiers at risk.

Attacking critical infrastructure: **Power, water, fuel, communications, commerse, and transportation** are all vulnerable to a cyber attack.

Compromised Counterfeit Hardware: Common hardware used in computers and networks that have **malicious software hidden inside the software, firmware, or even the microprocessors**.

The federal government of the United States admits that **the electric power transmission is susceptible to cyberwarfare** *(Tech, April 2008).*

The *U.S. Department of Homeland Security* works with industry, to identify vulnerabilities and to help industry enhance the security of control system networks. The federal government is also working to ensure that security is built in as the next generation of "smart grid" networks are developed *(Reuters: "U.S. Concerned Power Grid Vulnerable to Cyber Attack").*

In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national security officials *(Wall Street Journal, "Electricity Grid in U.S. Penetrated by Spies).*

The *North American Electric Reliability Corporation* (NERC) has issued a public notice that warns that **the electrical grid is not adequately protected from cyber attack** *(NERC Public Notice).*

China denies intruding into the U.S. electrical grid *(Xinhua: China Denies Intruding into the U.S. Electrical Grid, April 4, 2009; China Daily: China Threat Theory Rejected, April 4, 2009).*

One counter measure would be to disconnect the power grid from the internet and run the net with "droop speed control" only *(Disconnect Electrical Grid from Internet, Former Terror Czar Clarke Warns, Raw Story News, April 8, 2008).*

Massive power outages caused by a cyber attack could disrupt the economy, distract from a simultaneous military attack, or create a national trauma.

Howard Schmidt, the cyber security czar of the U.S., in an interview with *Wired* magazine, commented on those possibilities *(Wired magazine, March 4, 2010).*

The internet security company, *McAfee,* stated in their 2007 annual report that **approximately 120 countries have been developing ways to use the internet as a weapon and target financial markets, government computer systems, and utilities.** According to McAfee's George Kurtz, **corporations around the world face millions of cyber attacks a day.** "Most of these attacks don't gain any media attention or lead to strong political statements by victims" *("Google Attack Is Tip of Iceberg," McAfee Security Insights, January 13, 2010; "McAfee Cautions about Cold War-style Cyber Attacks," Top News, November 19, 2009).*

In its 2009 *Virtual Criminology Report*, the company cautioned that **"warfare can extend to the cyber arena—with countries like Russia, China, France, Israel, and the U.S. quietly involved in the process of expanding their computerized armory."** The experts involved in the report noted an increase in politically motivated online attacks, network infiltrations, and digital espionage.

McAfee VP Jeff Green writes of the threat:

"**Cyber crime is now a global issue. It has evolved significantly and is no longer just a threat to industry and individuals but increasingly to national security . . Attacks have progressed from initial curiosity probes to well-funded and well-organized operations for political, military, economic, and technical espionage**" *("Cyber Crime: A 24/7 Global Battle," McAfee, November 11, 2007).*

In 2007, *McAfee, Inc*., alleged that China was at the forefront of "cyberwar." **China was accused of cyber attacks on India, Germany, and the United States**, although they denied knowledge of these attacks. Arguments have been expressed regarding China's involvement. This indicates the methods of computer hackers who use zombie computers; it only shows that **China has the highest number of computers that are vulnerable to be controlled.** It is said that China has 75,000 zombie computers.

However, in a 2010 report by the U.S. Joint Forces Command, they noted that "Chinese discussions exhibit a deep respect for U.S. military power. There is a sense that **in certain areas, such as submarine warfare, space, and cyber warfare, China can compete on a near equal footing with America**" *("The Joint Operating Environment." Report released, February 18, 2010, pp. 34-36).*

Daniel Ventre notes that, **more and more frequently, accusations emerge which point toward China as being the source of major cyber attacks,** while admitting that it is difficult (or even impossible) to assert that the Chinese government and/or Chinese army are involved in the incidents assigned to them:

"These have reached sensitive targets, such as critical information infrastructures, the servers of big international firms and government agencies. The methods which are used in such "attacks" (not a clearly defined concept) are usually those of cyber criminals: intrusion, data theft, interception of data and communications, the spreading malwares and viruses, use of Botnets and web defacement. If cyber criminals are motivated by financial gains however, several of these attacks are not money-oriented operations. Some of them probably try to serve other goals, such as intelligence or the dissemination of ideologies."—*Daniel Ventre.*

But this much is known:

The People's Republic of China (PRC) has been and is currently utilizing a widespread effort to acquire U.S. military technology and classified information. In order to fulfill its long-term military development goals, the PRC uses a variety of efforts to obtain U.S. technology know-how. This includes **espionage; the exploitation of commercial entities; and a network of scientific, academic, and business contacts** *(deGraffenreid, Kenneth, ed.; The Unanimous and Bipartisan Report of the House Select Committee on U.S. National Security and Military Commercial Concerns with the People's Republic of China ["The Cox Report"], Select Committee, U.S. House of Representatives [Washington, D.C.: Regnery, 1999, p. 30]).*

The Chinese operate in ways that take advantage of U.S. judicial laws, so as to avoid prosecution. **The PRC uses a vast network of agents and contacts to collect pieces of information that is collated and put together in the PRC.** Often, each of the individual pieces is not enough to warrant any suspicion or prosecution from U.S. government personnel. **The aggressiveness of Chinese penetration is well-documented in multiple espionage cases—**including those of Larry Wu-Tai Chin, Katrina Leung, Gwo-Bao Min, Chi Mak, and Peter Lee. *(Global Security, "Ministry of State Security Operations." Wortzel, Larry M., Hearing on "Enforcement of Federal Espionage Laws." Testimony before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary, U.S. House of Representatives, January 29, 2008, pp. 6, 9).*

In addition to traditional espionage, **the PRC uses civilian companies to partner with American businesses in order to exploit advanced technology and economic data** *(Wortzel, p. 9).*

Additionally, **the PRC utilizes cyber espionage** to penetrate the computer networks of U.S. businesses and government agencies. This is evidenced by **a recent Chinese cyber attack on Google's computer systems** in December 2009 *(Helft, Miguel, and John Markoff, "In Rebuke of China, Focus Falls on Cyber Security," The New York Times, January 13, 2010).*

PRC intelligence operations in the United States have become so pervasive, **U.S. law enforcement officials have identified China as the most active foreign power involved in illegal acquisition of American technology** *(Wortzel, op. cit., page 8).*

U.S. Appoints First Cyber Warfare General: Pentagon creates specialist online unit to counter cyber attack amid growing fears of militarisation of the internet. Peter Beaumont, foreign affairs editor. The Observer, Sunday, May 23, 2010—

The U.S. military has appointed its first senior general to direct cyber warfare—despite fears that the move marks another stage in the militarisation of cyberspace.

The newly promoted four-star general, Keith Alexander, takes charge of the Pentagon's ambitious and controversial new Cyber Command, designed to conduct virtual combat across the world's computer networks. He was appointed on Friday afternoon in a low-key ceremony at Fort Meade, in Maryland.

The creation of America's most senior cyber warrior comes just days after **the U.S. air force disclosed that some 30,000 of its troops had been reassigned from technical support "to the frontlines of cyber warfare."**

The creation of Cyber Command is in response to increasing anxiety over the vulnerability of the US's military and other networks to a cyber attack.

James Miller, the deputy under-secretary of defence for policy, has hinted that **the US might consider a conventional military response to certain kinds of online attack.**

Although Alexander pledged during his confirmation hearings before the Senate committee on armed services last month that Cyber Command would not contribute to the militarisation of cyberspace, the committee's chairman, Senator Carl Levin, expressed concern that **both Pentagon doctrine and the legal framework for online operations had failed to keep pace with rapid advances in cyber warfare.**

In particular Levin voiced concern that US cyber operations to combat online threats to the US, routed through neutral third countries, "could have broad and

damaging consequences" to wider American interests.

Plans for Cyber Command were originally conceived under President George W. Bush. Since taking office Barack Obama has embraced the theme of cyber security, describing it last year as "one of the most serious economic and national security challenges [the US faces] as a nation."

During his confirmation hearing, Alexander said that **the Pentagon's networks were being targeted by "hundreds of thousands of probes every day"** adding that he had "been alarmed by the increase, especially in this year."

Cyber warfare has increased rapidly in scale and sophistication, with China accused of being at the forefront of prominent recent attacks, including the targeting of Google and 20 other companies last year as well as *"Titan Rain"* in 2003—a series of coordinated attacks on US networks. **Russian and North Korean hackers have also been accused of large-scale attacks.**

Moscow was accused of being behind a massive cyber assault on Estonia in 2007—the second largest cyber warfare operation ever conducted.

While Alexander has tried to play down the offensive aspects of his command, the Pentagon has been more explicit, stating on Friday that **Cyber Command will "direct the operations and defense of specified Department of Defense information networks** [involving some 90,000 military personnel] and prepare to, when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, [to] ensure US allied freedom of action in cyberspace, and deny the same to our adversaries."

The complex issues facing Cyber Command were thrown into relief earlier this year when the *Washington Post* revealed details of a so-called "dot-mil" operation by Fort Meade's cyber warfare unit, backed by Alexander, to shut down a "honeytrap website" set up by the Saudis and the CIA to target Islamist extremists planning attacks in Saudi Arabia.

The Pentagon became convinced that the forum was being used to co-ordinate the entry of jihadist fighters into Iraq.

Despite the strong objections of the CIA, the site was attacked by the Fort Meade cyber warfare unit. As a result, some 300 other servers in the Saudi kingdom, Germany, and Texas also were inadvertently shut down.

Of equal concern to those who had opposed the operation, it was conducted without informing key members of the Saudi royal family, who were reported to be "furious" that a counter-terrorism tool had been shut down.

The issue of cyber warfare—and how to combat it—has become an increasingly fraught one.

The need to have electronic warfare capabilities, say those who support them, has been proven repeatedly by the apparent success of hostile attacks on government networks, including last year's massive denial of service assault on networks in both the US and Korea.

Last year, hackers also accessed large amounts of sensitive data concerning the Pentagon's *Joint Strike Fighter program*.

The difficulties facing the new command were underlined in March by former CIA director Michael V. Hayden, who said that **the Saudi operation had demonstrated that cyber warfare techniques were evolving so rapidly that they were now outpacing the government's ability to develop coherent policies to guide its use.**

"Cyber was moving so fast that we were always in danger of building up precedent before we built up policy," Hayden said.

***U.S. Not Winning Cyber War, May 13, 2010. By Reuters, WASHINGTON*—The United States is losing enough data in cyber attacks to fill the Library of Congress many times over; and authorities have failed to stay ahead of the threat**, a U.S. defense official said on Wednesday.

More than 100 foreign spy agencies were working to gain access to U.S. computer systems, as were criminal organizations, said James Miller, principal deputy undersecretary of defense for policy.

Terrorist groups also had cyber attack capabilities.

"Our systems are probed thousands of times a day and scanned millions of times a day," Miller told a forum sponsored by Ogilvy Washington, a public relations company.

He said the evolving cyber threat had "outpaced our ability to defend against it."

"We are experiencing damaging penetrations—damaging in the sense of loss of information. And we don't fully understand our vulnerabilities," Miller said.

His comments came as the Obama administration develops a national strategy to secure U.S. digital networks and the Pentagon stands up a new military command for cyber warfare, capable of both offensive and defensive operations.

The Senate last week confirmed National Security Agency Director Keith Alexander to lead the new U.S. Cyber Command, which will be located at Ft. Meade, Maryland, the NSA's headquarters.