POLICY MEMO

January 2010

progressive
policy
institute
ppi

Spooks in the Machine:
How the Pentagon Should Fight Cyber Spies

by Noah Shachtman

In Washington, "cybersecurity" is a term that's come to have a thousand meanings, and none at all. Any crime, prank, intelligence operation, or foreign-government attack involving a computer has become a "cyber threat." Russian teenagers defacing Georgia's websites, hackers eyeing the power grid, overseas powers embedding government microchips with malicious code – they all share equal billing as cyber foes. The vague definition muddies the debate about what the real dangers are, where they lie, and how to respond to them. No wonder it took the White House so long to find someone to serve as a "czar" to coordinate government-wide responses. No wonder Congress is having such a hard time passing smart legislation.

But at the Pentagon, they aren't worried about some kid painting a Hitler moustache on Defense Secretary Robert Gates' online portrait. They're not even that concerned about a full-scale attack on the military's networks – even though the modern American way of war depends so heavily on the free flow of data. In the military, there's now broad agreement that one cyber threat trumps all others: electronic espionage, the infiltration (and possible corruption) of Defense Department networks. The Pentagon is seeking to coalesce around an organizational response, if not clear-cut answers, to the cyber-spying problem. But it's a very open question whether the solutions that they have come up with will make things better or worse for the military.

Well-placed spy software not only opens a window for an adversary to look into American military operations. That window can also be used to extract information – everything from drone video feeds to ammunition requests to intelligence reports. Such an opening also gives that enemy a chance to introduce his own false data, turning American command-

About the author
Noah Shachtman is a contributing editor at *Wired* magazine, and the editor of its award-winning national-security blog, "Danger Room."

and-control systems against themselves. How does a soldier trust an order, if he doesn't know who else is listening – or who gave the order in the first place? "For a sophisticated adversary, it's to his advantage to keep your network up and running. He can learn what you know. He can cause confusion, delay your response times – and shape your actions," says one Defense Department cyber official.[1]

Cyber spying on sensitive government networks isn't some theoretical concern. In December, we learned that militants could tap into the overhead surveillance feed of almost any aircraft in the American fleet – from spy drones to fighter jets.[2] The *Wall Street Journal* reported earlier this year that intruders were able to copy and siphon off "several terabytes of data" about the advanced F-35 Joint Strike Fighter stealth aircraft from the unclassified networks of defense contractor Lockheed Martin.[3] In 2008, USB "thumb drives" were used to slip malicious and self-replicating code onto military computers. According to a *60 Minutes* report, the software was able to monitor the classified networks of U.S. Central Command, which runs the American war efforts in Iraq and Afghanistan.[4] In 2007, the unclassified e-mail system of the Office of the Secretary of Defense was compromised.[5] Earlier in the decade, a researcher from Sandia National Laboratories caught Chinese cyber sleuths with specs for the U.S. Army's helicopter mission-planning system and for Falconview, the Air Force's aerial imagery software.[6]

The Problem of the Open Network

What's particularly vexing about these intrusions is that sophisticated methods weren't necessarily required to get inside the networks. In 2007, detailed schematics of Bagram Air Base in Afghanistan and the Camp Bucca detention facility in Iraq were downloaded by reporters from file transfer protocol servers with easy-to-find passwords or no protection at all.[7] The malware that spread via thumb drive across the military in 2008 had been around, in one form or another, since the early '90s.[8] In 2009, troops were so susceptible to virus- or Trojan-laden messages – supposedly sent from friends on Facebook and Twitter – that U.S. Strategic Command network security officers wanted to ban access to the social networks altogether.[9]

In other words, the end user – the service member or Pentagon civilian sitting at his desktop – is largely responsible for letting in these electronic intruders. They're the ones who set passwords to "1234," plug unknown drives into their computer, or download a Trojan virus when all they meant to do was sneak a peek at some online porn. "This makes us our own worst threat," writes one Department of Defense network security specialist. "There are a variety of reasons for this and most are tied to the collective DoD inability to mitigate known vulnerabilities – vulnerabilities users intentionally and unintentionally utilize to create adverse impacts or risks."[10]

The Pentagon spends millions of dollars every year on so-called "information assurance" – checking to see that military desktops are loaded only with trusted software, and reminding users not to respond to e-mails from Nigerians with dubious business propositions. But within the Defense Department, these are seen as Sisyphean tasks. "With seven million systems in the DoD, think how many idiots there are bound to be," one Pentagon cybersecurity official says.

The armed forces find it much easier to ban something than to educate its troops about responsible use. MySpace and YouTube are inaccessible from Pentagon computers – even though the military makes extensive use of the sites. Thumb drives are mostly forbidden as well, even though battlefield units rely on them to swap data in lonely places where bandwidth is hard to find. In the name of information security, information flow has been restricted. Meanwhile, secret overhead surveillance feeds are routinely left unencrypted; with an off-the-shelf satellite dish and $26 software, militants can see through the Air Force's eyes in the sky. It's a problem the military has known about for more than a decade but never bothered to fix. According to the *Wall Street Journal*, "the Pentagon assumed local adversaries wouldn't know how to exploit it."[11]

Clearly, there needs to be a rather serious re-evaluation of military information assurance. The Pentagon needs to do a better job of figuring out theoretical risks from actual dangers; secret drone feeds can't be left open while blogs are placed off-limits. Troops also need to be trained – and then trusted. The military routinely gives a 19-year-old private the power to kill everyone he sees. Surely, if that private can be taught to use an automatic rifle responsibly, he can be educated in computing without sharing secrets.

An Imperfect Solution

Now, many in the military are wondering whether an even more serious overreaction is in the works. In June, Secretary Gates established U.S. Cyber Command to coordinate all of the military's activities online. Heading the new command will be Lt. Gen. Keith Alexander, director of the super-secret National Security Agency (NSA). Conveniently for Alexander, the command will be located at Ft. Meade, Maryland – right next to the NSA's headquarters. The job of stopping electronic espionage, in other words, is being put in the hands of the military and intelligence outfit which is already responsible for snooping on e-mail, breaking electronic encryption algorithms, and sneaking into foreign networks. It has a logic: Our cyber spies will tackle their cyber spies. And few government agencies can rival the NSA's information security expertise.

> A great deal of today's most important cybersecurity research is being pursued at private companies and universities, from Microsoft to M.I.T. How well can a clandestine agency work with these unclassified groups?

But the move is problematic, too. For all of the NSA's brainpower, the agency has had its share of spectacular failures. It spent six years and $1.2 billion on the "Trailblazer" effort to sift through electronic communications, with little to show for it.[12] The successor project, "Turbulence," has proved problematic, as well.

The NSA's well-developed (some would say overdeveloped) sense of secrecy could also be an issue. Much of the country's network infrastructure is in private, not government, hands. A great deal of today's most important cybersecurity research is being pursued at private companies and universities, from Microsoft to M.I.T. How well can a clandestine agency work with these unclassified groups? Or even with military groups that might not be able to match the NSA's security clearances?

Finally, the NSA has a rich history of monitoring the communications of Americans – sometimes legally, sometimes not. Earlier this year, the Justice Department confirmed that the agency was still "overcollecting" on U.S. citizens, despite the wide latitude the NSA now enjoyed to spy on whom it likes. According to the *New York Times*, the agency even "tried to wiretap a member of Congress without a warrant."[13] Some in the armed forces cybersecurity community argue that in order to stop online espionage, the infiltrators need to be caught before they enter American networks. Cyberdefense becomes cyberoffense. With such a broad charter, the monitoring of innocent Americans' datastreams would only grow, with an agency well-known for privacy violations in charge.

Guard the Networks – or Live Without Them

Clearly, the NSA has a major role to play in the nation's network security. They've got the expertise that's lacking in the various armed services' geek squads, the network policy makers at U.S. Strategic Command's Joint Task Force Global Network Operations, and the Defense Information Systems Agency's cadre of Pentagon system administrators. But the NSA's role can't be all-encompassing. The agency needs to be part of a team. That team needs to include players that can work with experts both in and out of government. And that team needs to have oversight of the NSA's activities, so that citizens' civil liberties aren't slaughtered wholesale in the name of cybersecurity.

Other groups within the Pentagon are trying to make the armed forces more resilient in the face of cyber attacks. They not only want to make the military's data networks less susceptible to infiltration – they want to make its social connections more durable, too. If the military information grid is compromised, and orders can't be trusted, they want service members to be able to carry on with their missions regardless.

Troops can't lose time-honored skills just because they're in a digital age. They need to be able to navigate without electronic maps, assemble information without online databases, and distribute battle plans without e-mail. Some cybersecurity specialists say that more and more "redundant" networks need to be added in order to keep the military's data flowing. But for this group, the most important cyber defense may be learning to live without networks at all.

Noah Shachtman is a contributing editor at Wired magazine, and the editor of its national security blog, "Danger Room." He's reported from Afghanistan, Israel, Iraq, the Pentagon, and a couple of undisclosed locations, too. He's written about technology and national security for publications like The New York Times, The Chicago Tribune, and The Bulletin of the Atomic Scientists. The Associated Press, CNN, Fox News, MSNBC, and NPR have all asked him to provide insight on defense developments.

[1] Private interview, November 11, 2009.
[2] Siobhan Gorman, et. al. “Insurgents Hack U.S. Drones,” Wall Street Journal, December 17, 2009; Noah Shachtman, “Not Just Drones: Militants Can Snoop on Most U.S. Warplanes,” Wired.com’s Danger Room, December 17, 2009.
[3] Siobhan Gorman, et. al. “Computer Spies Breach Fighter-Jet Project,” Wall Street Journal, April 21, 2009.
[4] 60 Minutes, “Cyber War: Sabotaging the System,” November 8, 2009.
[5] Sharon Gaudin, “Hack Attack Forces Pentagon To Take Computers Offline,” Information Week, June 22, 2007.
[6] Nathan Thornburgh, “The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them),” Time, August 29, 2005.
[7] Mike Baker, “Sensitive military files readily available online,” Associated Press, July 11, 2007.
[8] Noah Shachtman, “Under Worm Assault, Military Bans Disks, USB Drives,” Wired.com’s Danger Room, November 19, 2008.
[9] Noah Shachtman, “Military May Ban Twitter, Facebook as Security ‘Headaches,’” Wired.com’s Danger Room, July 30, 2009.
[10] Private correspondence, November 11, 2009.
[11] Siobhan Gorman, et. al., “Insurgents Hack U.S. Drones,” Wall Street Journal, December 17, 2009.
[12] Siobhan Gorman, “Spy data system a ‘boondoggle’,” Baltimore Sun, January 29, 2006.
[13] Eric Lichtblau, and James Risen, “Officials Say U.S. Wiretaps Exceeded Law,” New York Times, April 15, 2009.

About the Progressive Policy Institute

The Progressive Policy Institute (PPI) is an independent research institution that seeks to define and promote a new progressive politics in the 21st century. Through research, policy analysis and dialogue, PPI challenges the status quo and advocates for radical policy solutions.

Progressive Policy Institute
1301 Connecticut Avenue
Suite 450
Washington, DC 20036

Tel 202.525.3926
Fax 202.525.3941
Email info@ppionline.org
www.progressivefix.com