

CYBERSPACE

Military wrestles with cyber war battle planning

Federal Computer Week, By: Ben Bain and Amber Corrin, July 26, 2010
<http://fcw.com/articles/2010/07/26/feat-cyber-command-tackles-cyber-war.aspx>

Many historians maintain that it was the ability to decipher Japanese code and not the creation of a new bruising battleship that turned the tide for the U.S. Navy in the Pacific theater during World War II. Meanwhile, in the Atlantic, Allied bombers tried to conceal their aerial attacks by dropping tiny strips of metal foil to sabotage German radar.

Militaries have long sought to seize the advantages and exploit the vulnerabilities that information technology brings to the battlefield. Now, more than ever, that duality of advantage and vulnerability sums up the U.S. military's deep dependence on IT.

The advanced weapons and communications systems that underpin U.S. military superiority rely on the uninterrupted functioning of that IT backbone and protection of the information it contains — a fact plainly understood by adversaries ranging from other nations to terrorist groups. Defense Department systems are probed by unauthorized users roughly 250,000 times an hour, or more than 6 million times a day, according to DOD officials.

the IT systems that form the backbone of the nation's industrial base play a similarly critical role, with similar vulnerabilities. To compound the challenge, the military, civilian sector and even adversaries use many of the same commercial computer products, which makes them a double-edged sword.

Yet when it comes to providing security in this complex new world of risks and opportunities, the military's past efforts have not been as well coordinated as they could have been. For example, their efforts have focused mostly on the defensive side of the equation.

DOD was "unorganized for the cyber threat for the 21st century," said Paul Kurtz, a cybersecurity expert who served on the White House's National Security and Homeland Security councils during the Clinton and George W. Bush administrations. But, Kurtz said, the military has come to the realization that "cyber weaponry would be a very important arrow in the quiver."

DOD publicly recognized its needs in that area in June 2009, and this past May, it activated the Cyber Command, which is part of the Strategic Command. Cybercom is intended to integrate and coordinate DOD cyber defenses that previously were based in the individual military services.

Led by Army Gen. Keith Alexander, Cybercom also oversees offensive cyber capabilities, and that involves developing weapons and the doctrine that governs when and how those weapons can be used. When he took command of Cybercom, Alexander retained his post as director of the nation's largest intelligence agency, the National Security Agency, which is responsible for signals intelligence and information assurance.

Besides resolving previous gaps and shortcomings, the creation of a command with that level of authority also recognizes the unique and important role of cyberspace.

“As a doctrinal matter, the DOD has declared this a domain, the cyberspace domain,” said Air Force Maj. Gen. Suzanne Vautrinot during a speech in Washington last month at a conference that Symantec hosted. Vautrinot is director of plans and policy at Cybercom. “This is the only [domain] that’s not controlled by God or Mother Nature, depending on your proclivities.”

It’s also a domain without precedent, which poses a challenge in setting objectives, organizational structures, resources and capabilities. Cyberspace involves air, space, land and sea, but it doesn’t fall neatly within any of them. As Cybercom moves into its third month, devising clear policies and rules of engagement is high on the to-do list.

Cyber Ops

Although the new command just came online, the military’s focus on cyberspace is hardly new.

Each of the services has or is in the process of setting up an operational cyberspace command. Alexander recently referred to the Army Forces Cyber Command, Marine Corps Forces Cyberspace Command, 24th Air Force and Navy’s Fleet Cyber Command as Cybercom’s boots on the ground. However, until now, those assets haven’t been controlled in a coordinated fashion.

One of Cybercom’s main objectives is to better integrate and coordinate those commands’ operations, Vautrinot said. It also includes the staffs from DOD’s Joint Functional Component Command for Network Warfare and the Joint Task Force-Global Network Operations.

Prescott Winter, a former chief technology officer and chief information officer at NSA, said there are long-standing concerns about cyber doctrine. He said those concerns hinge on having someone who could review all the options and understand how to coordinate available capabilities in the context of a larger military engagement.

“What you don’t want to do is start an operation and then suddenly discover that armed forces are tripping all over each other out there in cyberspace somewhere,” said Winter, now CTO of ArcSight’s public-sector business.

Cybercom’s creation is an effort to keep that from happening. As part of its mission, Cybercom plans, coordinates, integrates, synchronizes and conducts activities to defend DOD information networks and, when necessary, help conduct military cyberspace operations.

The last part of its mission statement refers to the ability to go on the cyber offensive, a mode of operation that many cybersecurity experts have long thought of as necessary, but one that is seldom discussed by DOD officials publicly or in detail. Cybercom’s launch hasn’t loosened many lips when it comes to talking about the tools in the United States’ offensive cyber arsenal.

“We’re doing what you would expect us to do,” said Navy Rear Adm. Michael Brown, deputy assistant secretary of cybersecurity and communications at the Homeland Security Department. “We’re developing a framework across the spectrum of conflict.”

Experts say cyber capabilities can allow the military to use computer keystrokes to achieve objectives that in the past required advanced weaponry or air power to accomplish.

For example, a cyberattack could include turning off an adversary’s power grid and then turning it back on later without needing to spend time and money to rebuild it, as would be the case if the military had used conventional weapons to destroy it.

“That’s certainly one attack that I think we’re likely to see in future conflicts because it’ll be much more surgical than even the smartest bomb,” said Robert Knake, an international affairs fellow in residence at the Council on Foreign Relations.

Knake and Richard Clarke, former counterterrorism adviser for Democratic and Republican presidential administrations, have co-authored a new book, “Cyber War: The Next Threat to National Security and What to Do About It.” In it, Knake and Clarke cite a 2007 incident in which they said Israel used light and electric pulses to control what Syrian air defense radar saw. That allowed Israeli aircraft to destroy a structure believed to be a clandestine nuclear facility.

Cybercom will likely have cyber weapons at its command that can similarly blur the line between offensive and defensive modes. In a military context, the difference between being able to probe and penetrate an adversary’s computer network or attack it comes down to a couple of keystrokes, Knake said.

Likewise, Kurtz, now a managing partner based in the United Arab Emirates for Good Harbor Consulting, said, “You can have a small piece of code that can do a whale of a lot of damage or just a little bit of damage depending on how you choose to use it.”

Just as important as the cyber weapons — offensive or defensive — are the people who will wield them. So organizing those human resources is also high on Cybercom’s agenda.

“Offense and defense are there at the same time, so you’ve got to plan a strategy in advance, you’ve got to be able to work as an integrated team being able to play with each other and recognize the talents and skills of the entire team,” Vautrinot said.

Others agree that properly managing the people will be crucial. “The big take-away here should be it’s about capability: how well trained, how disciplined, how broad is your capability within your offensive organization,” Knake said.

Uncharted Territory

Just as decades ago the military recognized the need for special skills to operate in the air, officials now understand that a specific skill set is necessary for cyberspace. In that context,

Cybercom's creation represents a logical progression, said Dan Kuehl, a military historian and professor of information operations at National Defense University's iCollege.

"This is a brand-new domain," he said. "We're learning how to do it. It's not the same as the other domains, and so the development of expertise and capabilities in this domain are best served not by burying it within some existing structure but by going to something new and unique."

Noah Shachtman, a nonresident fellow at the Brookings Institution and editor of Wired magazine's national security blog, "Danger Room," said it remains to be seen what the exact scope of Cyber Command's mission will be.

As Alexander noted during his confirmation hearing before the Senate Armed Services Committee in April, "We can stand up the command under existing authorities, but there is undoubtedly much uncharted territory."

Indeed, the command faces unprecedented questions about personnel, policy, law, doctrine and rules of engagement.

One vexing issue is the role the military should play in protecting private-sector networks if they come under attack, particularly a peacetime attack that originates abroad but is routed through computers owned by U.S. residents.

Alexander said that in such a scenario, DHS would lead because it has responsibility for critical infrastructure. But it could ask for and receive DOD's support. "If asked to do that, we'd get an execute order, and we'd have the standing rules of engagement that we operate under all the time," Alexander said. "The issues now, though, are far more complex because you have U.S. persons [involved]. Civil liberties, privacy — all come into that equation."

Another potential wrinkle, for privacy and operational issues, is the role of NSA, which Alexander also directs. NSA and Cybercom are located at Fort Meade, Md.

Alexander stressed during his confirmation hearing that there would be significant synergy between the two organizations, but each would have its own mission. "There will be two distinct staffs, with distinct authorities and responsibilities for how we operate for intelligence, for information assurance on the NSA side and, for Cyber Command, how we defend and secure our networks and conduct cyberspace operations if directed," he said.

For Knake, the most important question is how Cybercom officials will decide when to respond to state-sponsored cyber threats against civilians and companies. "What are the thresholds for the military to engage in offensive cyber activity in defense of the United States?" he asked. "That's really the biggest question: When should that take place?"

Even with clear rules, knowing whom to target with cyber operations will not be easy. A sophisticated adversary can make it nearly impossible to identify where a cyberattack came from.

“Attribution is a huge problem right now,” said Arthur Wachdorf, senior adviser for intelligence and cyber operations at the 24th Air Force, the service’s component command for Cybercom. “Attribution is inexorably linked to how we come up with these terms and policies dealing with attack, espionage or what we’re going to do about that. We have to be able to do it fast enough that it’s militarily relevant.”

None of these are easy questions, but Cybercom officials and supporters understand the challenges they face.

“The easy and simple stuff was done long ago,” Alexander said during a recent speech. “We got the rest.”