GlobalResearch
Center for Research on Globalization

CYBERSPACE: Pentagon Declares the Internet a "War Domain"

By John T. Bennett
Global Research, July 15, 2011
The Hill 15 July 2011

Region: USA
Theme: Militarization and WMD

The Pentagon released a long-promised cybersecurity plan Thursday that declares the Internet a domain of war.

The plan notably does not spell out how the US military would use the Web for offensive strikes, however.

The Defense Department's first-ever plan for cyberspace calls on the department to expand its ability to thwart attacks from other nations and groups, beef up its cyber-workforce and expand collaboration with the private sector.

Like major corporations and the rest of the federal government, the military "depends on cyberspace to function," the DoD plan says. The US military uses cyberspace for everything from carrying out military operations to sharing intelligence data internally to managing personnel.

"The department and the nation have vulnerabilities in cyberspace," the document states. "Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity."

Other nations "are working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD's information infrastructure," the plan states. "Moreover, non-state actors increasingly threaten to penetrate and disrupt DoD networks and systems."

Groups are capable of this largely because "small-scale technologies" that have "an impact disproportionate to their size" are relatively inexpensive and readily available.

The Pentagon plans to focus heavily on three areas under the new strategy: the theft or exploitation of data; attempts to deny or disrupt access to US military networks; and attempts to "destroy or degrade networks or connected systems."

One problem highlighted in the strategy is a baked-in threat: "The majority of information technology products used in the United States are manufactured and assembled overseas."

DoD laid out a multi-pronged approach to address those issues.

As foreshadowed by Pentagon officials' comments in recent years, the plan etches in stone that cyberspace is now an "operational domain" for the military, just as land, air, sea and space have been for decades.

“This allows DoD to organize, train and equip for cyberspace” as in those other areas, the plan states. It also notes the 2010 establishment of US Cyber Command to oversee all DoD work in the cyber-realm.

The second leg of the plan is to employ new defensive ways of operating in cyberspace, first by enhancing the DoD’s “cyber hygiene.” That term covers ensuring that data on military networks remains secure, using the Internet wisely and designing systems and networks to guard against cyberstrikes.

The military will continue its “active cyber defense” approach of “using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems.” It also will look for new “approaches and paradigms” that will include “development and integration … of mobile media and secure cloud computing.”

The plan underscores efforts long under way at the Pentagon to work with other government agencies and the private sector. It also says the Pentagon will continue strong cyber R&D spending, even in a time of declining national security budgets.

Notably, the plan calls the Department of Homeland Security the lead for “interagency efforts to identify and mitigate cyber vulnerabilities in the nation’s critical infrastructure.” Some experts have warned against DoD overstepping on domestic cyber-matters.

The Pentagon also announced a new pilot program with industry designed to encourage companies to “voluntarily [opt] into increased sharing of information about malicious or unauthorized cyber activity.”

The strategy calls for a larger DoD cyber-workforce.

One challenge, Pentagon experts say, will be attracting top IT talent because the private sector can pay much larger salaries — especially in times of shrinking Defense budgets. To that end, “DoD will focus on the establishment of dynamic programs to attract talent early,” the plan states.

On IT acquisition, the plan lays out several changes, including faster delivery of systems; moving to incremental development and upgrading instead of waiting to buy “large, complex systems”; and improved security measures.

Finally, the strategy states an intention to work more closely with “small- and medium-sized business” and “entrepreneurs in Silicon Valley and other US technology innovation hubs.”

The reaction from Capitol Hill in the immediate wake of the plan’s unveiling was mostly muted. Cybersecurity is not a polarizing political issue in the way some defense issues are, like missile defense.

Claude Chafin, a spokesman for House Armed Services Committee Chairman Buck McKeon (R-Calif.), called the strategy “the next step in an important national conversation on securing critical systems and information, one that the Armed Services Committee has been having for some time.”

That panel already has set up its own cybersecurity task force, which Chafin said would “consider this [DOD] plan in its sweeping review of America’s ability to defend against cyber attacks.”

As the Pentagon tweaks its approaches to cybersecurity, Senate Armed Services Committee ranking member John McCain (R-Ariz.) on Wednesday wrote Senate leaders saying that chamber must as well. McCain asked Majority Leader Harry Reid (D-Nev.) and Minority Leader Mitch McConnell (R-Ky.) to establish a temporary Select Committee on Cyber Security and Electronic Intelligence Leaks.

"Cybersecurity proposals have been put forth by numerous Senate committees, the White House and various government agencies; however, the Senate has yet to coalesce around one comprehensive proposal that adequately addresses the government-wide threats we face," McCain's office said in a statement. "A select committee would be capable of drafting comprehensive cybersecurity legislation quickly without needing to work through numerous and in some cases competing committees of jurisdiction."
