May 31, 2012 Wash. Post “U.S. Builds a Cyber ‘Plan X’” -- DARPA program

Key Messages:

- ***The U.S. is not militarizing cyberspace.***
- ***DoD tries to anticipate threats and potential means to address them.***
- ***Exploring opportunities to use cyberspace to protect the nation is a natural part of DoD’s responsibilities.***

Talking Points:

- The 2010 *Defense Strategy for Operating in Cyberspace* emphasized how important it is for the U.S. military to operate effectively in cyberspace.

- DoD is investing aggressively to develop new capabilities for cyberspace activities because DoD’s networks are being threatened every day:

    - Improved capabilities to defend;
    - Improved capabilities for situational awareness;
    - Improved capability to use cyberspace for offensive activities, if directed.

- DARPA's activities are just one of many efforts in these areas.

- Operations that utilize cyber capabilities will be approved at senior levels of DoD and the Administration. DoD has authority to conduct the full range of cyber operations to defend U.S. national security, as directed by the President.

- The President can use any DoD capability, or combination of capabilities, to respond to threats to our nation, including cyber threats.

Questions and Answers:

Q: What other offensive and defensive cyber capabilities is DARPA developing?

A: DoD does not discuss specific capability requirements in this area. DARPA’s efforts are part of the Department’s commitment to develop capabilities to conduct full spectrum cyber operations to defend U.S. national security interests.

Q: Is DARPA’s Plan X a response to another organization/nation’s similar capabilities?

A: No. DARPA's activities are just one of many DoD efforts to improve our ability to address existing and emerging cyber threats.

Q: During the "speed-of-light attacks" described in the Washington Post article, who will have command and control if human operators are not involved?

A: There will always be senior level approval to employ cyber capabilities.

Washington Post
May 31, 2012
Pg. 1

U.S. Builds A Cyber 'Plan X'

Effort to boost war capabilities; Research push marks new offensive phase

By Ellen Nakashima

The Pentagon is turning to the private sector, universities and even computer-game companies as part of an ambitious effort to develop technologies to improve its cyberwarfare capabilities, launch effective attacks and withstand the likely retaliation.

The previously unreported effort, which its authors have dubbed Plan X, marks a new phase in the nation's fledgling military operations in cyberspace, which have focused more on protecting the Defense Department's computer systems than on disrupting or destroying those of enemies.

Plan X is a project of the Defense Advanced Research Projects Agency, a Pentagon division that focuses on experimental efforts and has a key role in harnessing computing power to help the military wage war more effectively.

"If they can do it, it's a really big deal," said Herbert S. Lin, a cybersecurity expert with the National Research Council of the National Academies. "If they achieve it, they're talking about being able to dominate the digital battlefield just like they do the traditional battlefield."

Cyberwarfare conjures images of smoking servers, downed electrical systems and exploding industrial plants, but military officials say cyberweapons are unlikely to be used on their own. Instead, they would support conventional attacks, by blinding an enemy to an impending airstrike, for example, or disabling a foe's communications system during battle.

The five-year, $110 million research program will begin seeking proposals this summer. Among the goals will be the creation of an advanced map that details the entirety of cyberspace - a global domain that includes tens of billions of computers and other devices - and updates itself continuously. Such a map would help commanders identify targets and disable them using computer code delivered through the Internet or other means.

Another goal is the creation of a robust operating system capable of launching attacks and surviving counterattacks. Officials say this would be the cyberspace equivalent of an armored tank; they compare existing computer operating systems to sport-utility vehicles - well suited to peaceful highways but too vulnerable to work on battlefields.

The architects of Plan X also hope to develop systems that could give commanders the ability to carry out speed-of-light attacks and counterattacks using preplanned scenarios that do not involve human operators manually typing in code - a process considered much too slow.

Officials compare this to flying an airplane on autopilot along predetermined routes.

It makes sense "to take this on right now," said Richard M. George, a former National Security Agency cyberdefense official. "Other countries are preparing for a cyberwar. If we're not pushing the envelope in cyber, somebody else will."

Military initiative

The shift in focus is significant, said officials from the Pentagon agency, known by the acronym DARPA. Cyber-operations are rooted in the shadowy world of intelligence-gathering and electronic-spying organizations such as the NSA.

Unlike espionage, military cyberattacks would be aimed at achieving a physical effect - disrupting or shutting down a computer, for example - and probably would be carried out by the U.S. Cyber Command, the organization that was launched in 2010 next to the NSA at Fort Meade.

"Because the origins of cyberattack have been in the intelligence community, there's a tendency to believe that simply doing more of what they're doing will get us what we need," said Kaigham J. Gabriel, acting director of DARPA. "That's not the way we see it. There's a different speed, scale and range of capabilities that you need. No matter how much red you buy, it's not orange."

Plan X is part of a larger DARPA effort begun several years ago to create breakthrough offensive and defensive cybercapabilities. With a cyber budget of $1.54 billion from 2013 to 2017, the agency will focus increasingly on cyber-offense to meet military needs, officials say.

DARPA's research is designed to foster long-shot successes. In addition to helping create the Internet, the agency's work gave rise to stealth jet technology and portable global-positioning devices. "Even if 90 percent of their ideas don't pan out," said Martin Libicki, a cyberwar expert at Rand Corp., "the 10 percent that are worthwhile more than pay back the difference."

A digital battlefield map, as DARPA envisions it, would plot nodes on the Internet, drawing from a variety of sources and changing as cyberspace changes.

"In a split microsecond you could have a completely different flow of information and set of nodes," Gabriel said. "The challenge and the opportunity is to create a capability where you're always getting a rapid, high-order look of what the Internet looks like - of what the cyberspace looks like at any one point in time."

The ideal map would show network connections, analyze how much capacity a particular route has for carrying a cyberweapon and suggest alternative routes according to traffic flows, among other things.

The goal would be a visual representation of cyberspace that could help commanders make decisions on what to attack and how, while seeing any attacks coming from an enemy.

Achieving this will require an enormous amount of upfront intelligence work, experts say.

Michael V. Hayden, a former NSA director and a former CIA director, said he can imagine a map with red dots representing enemy computers and blue dots representing American ones.

When the enemy upgrades his operating system, the red dots would blink yellow, meaning the target is out of reach until cyber operators can determine what the new operating system is.

"I can picture that," Hayden said. "But this really is bigger than all outdoors."

Complicated controls

Plan X also envisions the development of technology that enables a commander to plan, launch and control cyberattacks.

A commander wanting to hit a computer that controls a target - a strategically important drawbridge in enemy territory, for example - should be able to predict and quantify battle damage while considering the timing or other constraints on a possible attack, said Dan Roelker, Plan X program manager.

Cyberwar experts worry about unintended consequences of attacks that might damage the flow of electricity to civilian homes or hospitals. A targeting system also should allow operators to stop a strike or reroute it before it damages systems that are not targeted - a fail-safe mechanism that experts say would be very difficult to engineer.

DARPA will not prescribe what should be represented on the digital map.

Some experts say they would expect to see power and transportation systems that support military objectives.

Daniel Kuehl, an information warfare professor at the National Defense University's iCollege, said the Air Force built its history around attacks on infrastructure - in Korea, Vietnam, Serbia and Iraq.

"In all of those conflicts," he said, "we went after the other side's electricity with bombs."

Today, he said, cyberweapons could be more humane than pulverizing power grids with bombs.

If a cyberwarrior can disrupt a computer system controlling an enemy's electric power, the system theoretically can also be turned back on, minimizing the impact on civilians.

But retired Gen. James E. Cartwright, who as vice chairman of the Joint Chiefs of Staff until August pushed to develop military cyber-offense capabilities, said the military is focused less on power grids than on "tanks and planes and ships and anything that carries a weapon."

"The goal is not the single beautiful target that ends the war in one shot. That doesn't exist," said Cartwright, who is now with the Center for Strategic and International Studies. "The military needs more of a brute-force approach that allows it to get at a thousand targets as quickly as possible. "