The Hunt for the New Duct Tape – New Defense Cyber Strategy Looks to Cyber R&D

Posted At : May 13, 2015 4:35 PM | Posted By : John Slye
Related Categories: Critical Infrastructure Protection, Department of Defense, Technology Trends, Innovation, Information Security, Air Force, Army, Cybersecurity

The Secretary of Defense, Ashton Carter, announced last week the release of the Department of Defense's (DoD) new Cyber Strategy aimed at improving the their cyber capabilities. One theme focuses on leveraging cybersecurity research and development (R&D) to accelerate these capabilities. So how much money might DoD be directing toward cyber R&D?

New Defense Cyber Strategy – Overview

The stated purpose of the new *Department of Defense Cyber Strategy* is to guide the development of DoD's cyber forces and strengthen its cyber defense and cyber deterrence posture. The strategy focuses on building cyber capabilities and organizations for DoD's three cyber missions: defend DoD networks, systems, and information; defend the United States and its interests against cyberattacks of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans.

The strategy sets five strategic goals and establishes specific objectives for DoD to achieve over the next five years and beyond.

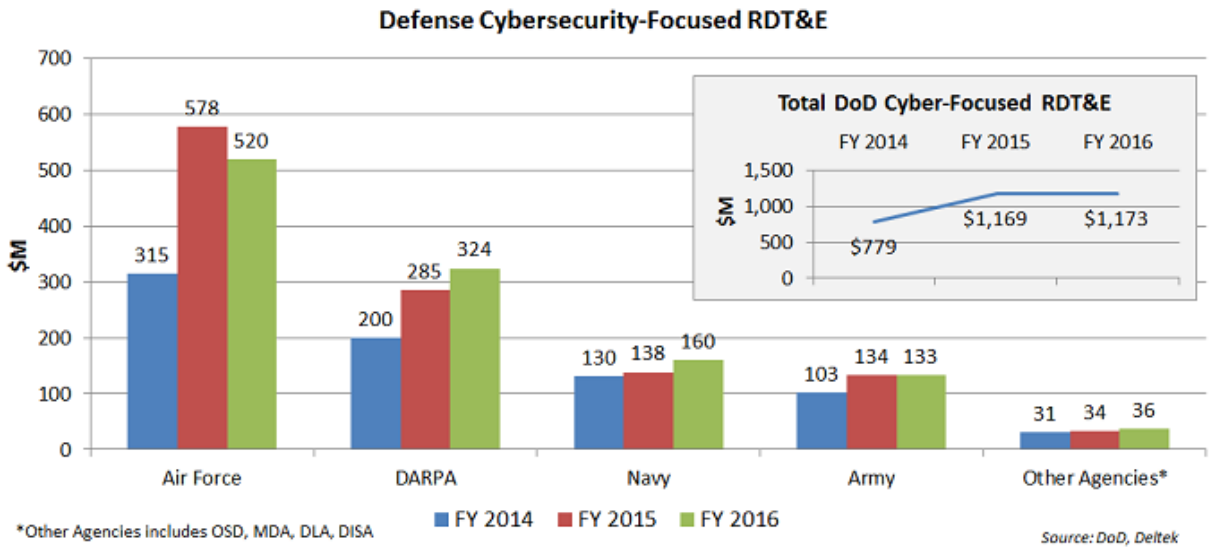
1. Build and maintain ready forces and capabilities to conduct cyberspace operations
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability

Cybersecurity Research and Development

Under the first strategic goal in the area of *building technical capabilities for cyber operations* the DoD is setting an objective to *accelerate innovative cyber research and development* (R&D) to build their cyber capabilities, looking to both the existing DoD R&D community and to established and emerging private sector partners for help in developing "leap-ahead technologies" that can aid U.S. cyber-defenses. To that end, DoD plans to focus its basic and applied R&D on developing cyber capabilities to expand the capacity of overall cyber workforce.

What might cyber-focused R&D look like in budgetary terms across the DoD? Looking at the FY 2016 Defense Research, Development, Test and Evaluation (RDT&E) budget books gives a general sense of magnitude and relative distribution of recent and proposed budget dollars. Reviewing the various RDT&E budget artifacts for Army, Air Force, Navy, and the Defense Agencies and searching for key terms like *cybersecurity, information assurance,* and *information security* identifies dozens of programs that are *primarily directed* at cybersecurity (and several more that appear cybersecurity-*related*.)

Looking at just the programs that appear *directly* cybersecurity-focused in the FY 2016 DoD RDT&E budget shows that the department budgeted nearly $780 million in FY 2014, with that level increasing to more than $1.1 billion in FY 2015 and FY2016. Further, the Air Force and DARPA have been the major players in the cyber R&D area for DoD, accounting for $844 million (72%) of the total $1.17 billion in FY 2016 requested funding. (See chart below.)



Implications

The R&D dollars depicted above are just part of the story. There is other cyber-related R&D spending embedded in larger efforts that contain cybersecurity elements or impacts, but ferreting out those dollars is gets tricky and can be even more imprecise. The point here is to get a sense of the size of the overall investment and where these dollars tend to be directed.

While it is important to recognize that not all of these dollars will be spent on contracts with industry partners for R&D services and technologies, the fact remains that the sustained need by DoD for more advanced cyber technologies and tools is likely to grow in both real terms and in proportion to other R&D areas. In fact, the investment in this push for greater cyber tools may easily outpace the growth rate for other areas of contractor-addressable cybersecurity within DoD. This is especially true in the support services area as the DoD strives to develop thousands of uniformed cybersecurity personnel in the coming years.

One thing seems for certain, the DoD recognizes its need to cover a lot of ground quickly when it comes to improving its cybersecurity capabilities and posture and they are looking to harness creative energies to address the need. In many ways, it's not unlike past challenges where they have looked to partners in industry and elsewhere to come up with creative solutions. Who knows? Soon we could be looking at the cyber equivalent of duct tape.