

Solutions for Mission Success: New Approaches to Weapon Systems Cybersecurity

A **FOREIGN POLICY** DEFENSE & NATIONAL SECURITY ROUNDTABLE SPECIAL REPORT

TECHNICAL PARTNER

Booz | Allen | Hamilton®

March 21, 2019

True cybersecurity in weapon systems requires new ways of thinking, ranging from looking at cybersecurity through a mission lens, to using a common language, to building a pipeline of cyber talent and expertise. Those were just a few of the important insights that emerged at the recent roundtable on cybersecurity for weapon systems, convened by *Foreign Policy* in partnership with Booz Allen Hamilton.

Participants in the roundtable included senior leaders in the Office of the Secretary of Defense (OSD), representatives of the Joint Staff, the Services, the U.S. Cyber Command and a federally funded research and development center (FFRDC), as well as senior leaders from Booz Allen.

As roundtable participants noted, what makes modern U.S. military weapons so lethal – automation and connectivity – is precisely what makes them more vulnerable to cyberattacks. Balancing that potency and vulnerability, they said, can be difficult. Many weapon systems functions are carried out by complex systems comprised of control systems and embedded IT. And because those systems rely on different architectures, interfaces and protocols than do traditional IT, it can be particularly challenging to protect them, and achieve cyber resilience, with conventional cybersecurity tools and approaches.

THE IMPORTANCE OF A MISSION FOCUS

Several roundtable participants suggested that the key to cybersecurity is treating it as a function of operational and mission readiness. The true test, they said, is not whether particular weapon systems or platforms are cyber secure, but rather whether the mission itself – both defensively and offensively – can be carried out in the face of a debilitating cyberattack. Getting such a clear mission focus isn't always easy – but it's critical to making the right decisions about cybersecurity funding and priorities, several participants said.

"I think the challenge is recognizing that networks are warfighting platforms," said one participant. "And until we more broadly take ownership of the fact that this is how we fight – by sharing data – we're going to be challenged." Said another participant: "This is a warfighting issue, and we're not treating it like a warfighting issue."

Another key aspect of mission focus is the issue of legacy systems. As several participants noted, the vast majority of the current weapon systems are legacy, rather than in development – and yet there's not nearly enough funding to address all of their vulnerabilities. Thinking about those vulnerabilities from a mission standpoint, several participants suggested, can help organizations determine which are most critical. That approach, they said, can guide

defense organizations as they carry out the mandate of Section 1647 of the FY 2016 National Defense Authorization Act, which requires the evaluation of cyber vulnerabilities of major Department of Defense (DoD) weapon systems.

At the same time, there is often a conflict over whether available funding should go toward enhancing the functionality of the weapon system or enhancing its cybersecurity. Looking at that question in terms of mission success can help achieve consensus in funding priorities, some participants said.

MOVING BEYOND COMPLIANCE

Roundtable participants acknowledged that it can be difficult to sufficiently address cybersecurity risk, and they sought to identify some of the reasons why. One factor, several said, is that there's often a tendency to focus on cyber compliance, rather than on the ultimate test – whether the weapon systems can do their jobs in a cyber-contested environment. In some cases, commanders don't have the funding, time or incentive to go beyond compliance. However, said one participant, "Compliance doesn't equal cybersecurity, and cybersecurity doesn't assure mission success." He added: "We've seen systems that are actually secure – but they're not operationally ready, or they don't actually get the mission done."

Said another participant, "There are hundreds, if not thousands of vulnerabilities on each and every one of our weapon systems, and there's no way we can afford to fix them all...very few of the weapon systems we have out there today are doing any real mitigation effort because they've got their ATO (authorization to operate), and that was their only cybersecurity or cyber survivability requirement. Until they lose that ATO, there's no incentive to spend \$1 to increase the cyber survivability." The participant said his organization is looking at new approaches that call for defining cyber survivability in critical weapon systems, and then allocating funding to buy down the risk of their known and unknown vulnerabilities.

Another challenge, participants said, is the language

gap between the warfighting and cyber realms. "Translating individual system vulnerabilities up to the mission level is hard," one participant said. "We understand what the term cybersecurity means, but we don't use terms like security in any other warfighting domain – we talk about hardness, lethality, survivability. We have to be mindful of the fact that the people who have to make the decisions are warfighters – and we have to describe what we need in cybersecurity, and why, in warfighting terms. If you can tell a combatant commander that he has a mission at risk, that's something he cares about."

Participants noted that the cyber attack surface for weapon systems is vast and complex, extending well beyond weapon systems and subsystems to include the many support systems that modern weapon systems connect to, such as maintenance, diagnostics, communications and command and control. Importantly, this includes installations and their support systems. As one participant said, "We fight from our installations."

THE VALUE OF WARGAMING

Weapon system cybersecurity requires a comprehensive knowledge of the mission, the adversary threat landscape, and the security architecture of the weapon system, including its critical dependencies and potential vulnerabilities. Defense organizations can bring these together, participants suggested, through approaches such as testing, exercises and wargaming.

For example, organizations can use wargaming to not just look at the cybersecurity of a particular weapon system, but to determine how the larger mission can be performed in a cyber-contested environment. "The way we're using the wargames is to help the combatant commanders understand the risks to their mission, so they'll be in a position to advocate for the people who write the checks," said one participant. "The objective is to develop a compelling evidence base that the combatant commanders can use to help make their cases for the services to say, 'Hey, you don't necessarily have to fix every system, but these systems need to be mitigated.'"

“CYBER DEFENSE TAKES A VILLAGE”

Roundtable participants emphasized another key theme – the importance of providing the military with a pipeline of people and expertise to help solve today’s pressing cybersecurity challenges. “I question if we have the right people on the bus,” said one participant. “I don’t care where you get them, but they’re out there, and they’re smart.” Said another participant, “Cyber defense takes a village.”

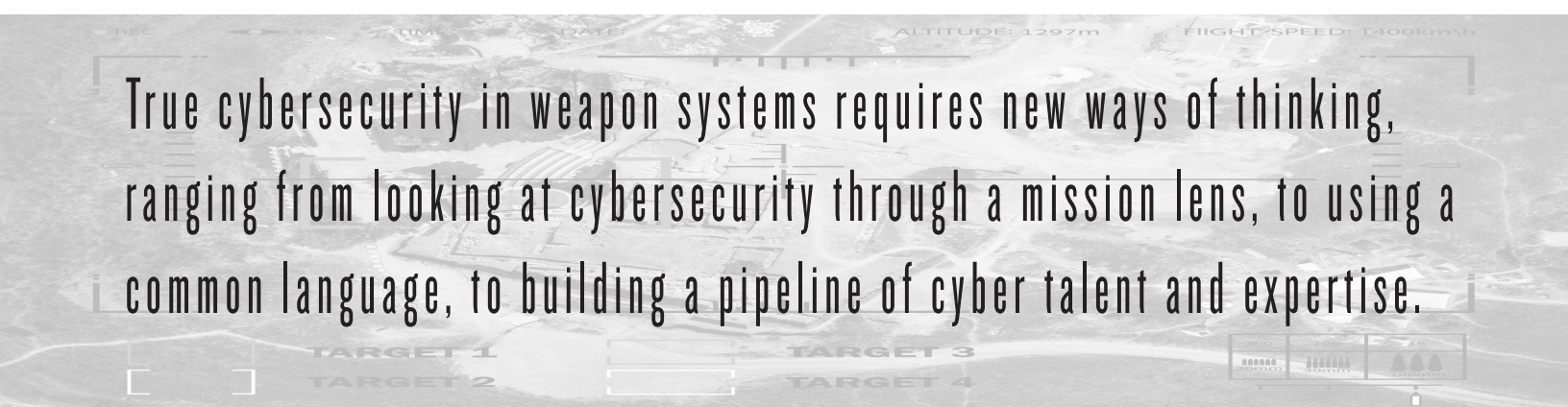
Participants also noted that people with PhDs in data science and artificial intelligence are needed as professors – but many are going into private industry because it pays so much more. “You can’t solve your problems if none of the PhDs are going into academia and teaching the next generation,” one participant said. “We need researchers, not just product developers.”

In the 1950s and 1960s, said another roundtable participant, there were about 20 scientists and technologists around the world – including in the U.S. – for each one in the DoD. “Today, this ratio stands between 500 to 1,000, and keeps growing. It’s not going to get any better and we better wake

up and realize that. The solution has to include our ability to interface with scientists and technologists around the world – including, of course, all the non-U.S. citizens who constitute the majority of computer scientists in our own country and abroad. How to do that? We need to learn how to use their talents, how to work with all those companies, and how to buy foreign-made technologies and make them usable for our military purposes.”

GAINING A COMMON UNDERSTANDING

One participant summed up the overall weapon systems cybersecurity challenge by saying, “This is a very complex problem. It’s not just a DoD problem, it’s a whole-of-government, all-of-the-United-States issue. We all have to have a common language, and a common understanding, of what we’re trying to solve.”



True cybersecurity in weapon systems requires new ways of thinking, ranging from looking at cybersecurity through a mission lens, to using a common language, to building a pipeline of cyber talent and expertise.

ROUNDTABLE ATTENDEES

- Chad Acey - Senior Cyber Advisor, US Army Intelligence and Security Command
- Jandria Alexander - Director and Lead, Cyber Weapon Systems and Platforms, Booz Allen Hamilton
- Katie Arrington - Special Assistant to the Assistant Secretary of Defense for Acquisition for Cyber across Acquisition & Sustainment
- Chris Bogdan - Senior Vice President and Lead, Aerospace, Booz Allen Hamilton
- Claire Casey - Managing Director, Foreign Policy Analytics
- Kevin Coggins - Vice President and Lead, Positioning, Navigation and Timing (PNT), Booz Allen Hamilton
- Major General Vincent Coglianesse - Commander, Marine Corps Installations Command/Assistant Deputy Commandant, Installations & Logistics (Facilities)
- Jeremy Epstein - Deputy Division Director, Computer & Network Systems Division, National Science Foundation
- John Garstka - Director for Cyber, Office of the Secretary of Defense, Acquisition and Sustainment
- Elias Groll - Staff Writer, Foreign Policy
- Amanda Hardgrave - Deputy Chief of Staff & US Coast Guard Military Advisor, Office of Net Assessment
- Frank Konieczny - Air Force Chief Technology Officer, Office of the Deputy Chief Information Officer, Office of the Secretary of the Air Force
- Charles Kosak - Deputy Assistant Secretary, Defense Continuity and Mission Assurance
- Alex Kott - Chief Scientist, Network Science Division, Army Research Lab
- Megan Lamberth - Research Assistant, Technology and National Security Program, Center for New American Security
- Sheryl Lyon - Command Sergeant Major, US Army Cyber Command
- Dale Ormond - Principal Director, Research, Office of the Assistant Secretary of Defense, Research and Engineering
- Steve Pitcher - Senior Cyber Survivability Analyst, The Joint Staff Army (J6)
- Alex Romero - Chief Information Security Officer, Defense Digital Service, Office of the Secretary of Defense
- Andrew Sollinger - Publisher, Foreign Policy
- Jonathan Tepperman - Editor in Chief, Foreign Policy
- Jack Wilmer - Deputy Chief Information Officer for Cybersecurity
- Ali Wyne - Policy Analyst, RAND Corporation