VULNERABILITY IN CYBERSPACE

By Will Skowronski, Senior Editor

Planners must ensure credible cyber defenses are present all through military systems.

Recent high-profile national cyber attacks show that everyone is vulnerable to the threat—including the Air Force. Unfortunately, like much of the world, USAF isn't properly organized or equipped to defend against dedicated cyber attacks, Gen. John E. Hyten, chief of Air Force Space Command, said during AFA's 2016 Air, Space & Cyber Conference in September.

Hyten said the 50th Space Wing at Schriever AFB, Colo., has mission defense teams looking at defending the service's capabilities across the board, "and holy cow, have we learned from our airmen as we've given them the responsibility to defend our weapons systems," he said.

While the service's cyber protection teams do have the equipment to defend weapons systems, he said, they take those tools or capabilities with them when they leave a particular wing or mission group. This is a problem that has to be addressed, said Hyten, who was confirmed, a week following the AFA conference, to head US Strategic Command.

Cyber attacks are "as much a threat to us in terms of our ability to effectively perform our mission as any of the other … tools that our adversary can use," Gen. Ellen M. Pawlikowski, commander of Air Force Materiel Command, said. "Our weapons systems are not totally invulnerable because they are not necessarily connected to the web when they're executing their mission."

NO EASY FIX

The wide range of threats—from losing control of a weapon-carrying remotely piloted aircraft, to plug-in equipment infecting a fighter jet's software, or simply a power outage at a base that powers cyber or space weapons—means there's no easy fix.

"There is no 'one size fits all' when it comes to our wings," Hyten said. "Every wing is different. … We need to be able to look at all of those wings and understand what we have to do."

Pawlikowski said the service has recognized its weapons systems are vulnerable to cyber attacks for years, but has taken little action to defend them.

"We spent a couple years … acting like Chicken Little and really didn't do anything to get at this issue of our weapons systems," Pawlikowski said. While almost everyone has been trained on network security, "we never really took a look at, 'What do we do about this? How do we deal with this?' "

In January 2015, a number of Air Force organizations, including Space and Missile Systems Center, AFMC, and acquisition, created a cyber resiliency steering group to understand the threat and think of ways to counter it.

The effort might have arrived just in time. US Cyber Command, which monitors the array of cyber threats to military assets, is beginning to see attempts to attack and take control of networks, rather than merely attempts to steal information, USAF Lt. Gen. James K. McLaughlin, CYBERCOM's deputy commander, said during the conference.

"It's really a different military problem," he asserted.

Last year, USAF's cyber resiliency group devised a campaign plan that may take up to seven years, with seven areas of focus: analyze mission threads to find potential cyber vulnerabilities; "bake in" cybersecurity to future weapons systems and upgrades; develop the needed cyber expertise; make weapons systems more flexible so cyber defenses can be upgraded;

establish a common understanding of the problem and common vocabulary for cyber security entities; reduce the vulnerability of legacy weapons systems; and collect intelligence on real-world threats.

Pawlikowski said although a lot of time has been spent on building the team of experts needed to implement these seven "lines of attack," it has made progress on each focus area. It has spent the last year—with the help of RAND Corp., MITRE Corp., and industry partners—beginning the work of mapping mission threads and analyzing vulnerabilities.

The mission-thread approach provides a situational awareness that other approaches might not, Pawlikowski said. As an example, she explained the multiple steps required to carry out an F-16 precision strike, many having no direct connection to flying the aircraft or launching weapons. These involve automatic test equipment used for maintenance or the system for uploading operational flight programs, each creating software connections to the aircraft—and thus cyber vulnerabilities. Planners need to consider these ancillary connections.

"When you look through and you lay out the mission thread that it takes to conduct a global precision attack, you find that there are cyber threat 'surfaces,' as I like to call them, all over the place," she said.

The best way to prevent attacks in the future, Pawlikowski said, is to address cybersecurity as early as possible in the life cycle of a weapon and make sure cyber defenses are included at the outset.

"We don't want to have to scab it on," she said.

The goal is to provide each necessary player—including contractors, government engineers, financial managers, and acquisition managers—the tools and knowledge to understand how to carry out a cyber risk assessment, then develop a test and evaluation master plan that includes cyber testing, Pawlikowski said. Cyber requirements will also be built into a program's contracts.

This cybersecurity effort will require recruiting and developing cyber experts and engineers.

"Tools are no good without the craftsmen that know how to use them," she said.

To that end, the Life Cycle Management Center is standing up an engineering team that will support all USAF program offices in developing cybersecurity measures as any given system moves through acquisition. The team will develop training programs and classes for people throughout the Air Force.

LINES OF ATTACK

Even designing systems for cyber security from the outset won't be enough, as threats will change faster than the pace of recapitalization. Accordingly, the fourth "line of attack" calls for building flexible, agile, and adaptable weapon systems with the use of open architecture and other means so platforms can be constantly upgraded to meet new threats.

"We have to be able to respond quickly," Pawlikowski said. As an example, "we can't take 10 years to change out the GPS positioning, navigation, and timing equipment in an airplane if there's [already] a cyber threat that has been able to negate our ability to use GPS."

To ensure the cyber campaign can be carried out across a program's life cycle, she said, USAF needs a classification guide and vocabulary that will establish a common understanding, because the current grasp of the security environment is scattershot.

Flexibility, agility, and adaptability depend on the cyber language to be "universally consistent," she said.

While planners want to bake in security measures in future weapons systems, the cyber campaign's sixth line of approach requires finding fixes for places where legacy systems are vulnerable.

Air Force Research Laboratory is working with industry partners to find the "biggest threat surfaces" and ones that appear in multiple mission threads so they can be closed with available resources first, Pawlikowski said. The most cost-effective approach will employ a combination of hardening cyber defenses while making systems resilient enough to fight through a cyber attack.

All system automated defenses will be supplemented by local defense teams.

"This is a combination of man-in-the-loop and building cyber resiliency," she explained. "One of the things that we've learned over the years," she said, is that trying to create comprehensive, automatic self-protection methods for weapon systems, "particularly ones that have a lot of threat surfaces," forces a reliance on software hardening that "can cause us to break the bank and not be very effective." Realistically, "when we look at introducing solutions to cyber protection, … it's not all on our industry partners to harden this thing so it's impenetrable."

Pawlikowski said she expects each USAF base will have a cyber operator to defend on-site weapon systems between 2020 and 2025.

Hyten said there are plans to assign each operations group a cybersecurity squadron, charged with defending systems, within 10 years.

The best way to prevent attacks in the future, Pawlikowski said, is to address cybersecurity as early as possible in the life cycle of a weapon and make sure cyber defenses are included at the outset.

But while planners can try to anticipate potential vulnerabilities, monitoring real-world cyber attacks is the only way to understand the true threat.

"We need to have cyber intelligence as part of this solution," Pawlikowski said while describing the seventh line of attack. "We can't try to defend against whatever our own creativity says we can do. We have to have intelligence."

She added that none of the interrelated lines of attack require technological breakthroughs to carry out.

"This is all just plain hard work," she said. "This is all just digging in, using the tools that we have, and putting the focus on it." ✪