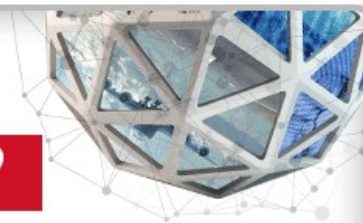


WHAT IS THE INFRASTRUCTURE SIDE OF CYBER?



[READ ARTICLE](#)

Raytheon

DoD

Securing the cockpit: How the military is tackling avionics cybersecurity

By: **Eric Tegler** 5 days ago



"We're realizing that the vulnerability is not just the networks. We have a lot of little closed networks internal to weapons systems that we didn't think of as networks or as something that might have cyber vulnerability," Col. Gregory Breazile, director of the C2/Cyber and Electronic Warfare Integration Division of the Marine Corps Cyber Task Force, told an audience at the 2015 CyberCon conference in Washington, D.C.

The threat of cyber interference with American military information systems is well known and intuitively understood. But until recently, the cyber threat to systems on individual platforms, particularly aircraft, had received comparatively little attention.

EVO PDF Tools Demo

In 2015, Col. Gregory Breazile, director of the C2/Cyber and Electronic Warfare Integration Division of the Marine Corps Cyber Task Force, speaking to an audience at that year's CyberCon conference in Washington, D.C., said, "We're realizing that the vulnerability is not just the networks. We have a lot of little closed networks internal to weapons systems that we didn't think of as networks or as something that might have cyber vulnerability."

Breazile's comments reflected recognition that the avionics — weapons as well as position, navigation and timing systems — embedded in U.S. military aircraft and other platforms are vulnerable. But how vulnerable?



[EXPLORE](#)

Raytheon

Quick Links

[Newsletters](#)

[Whitepapers](#)



[EXPLORE](#)

Raytheon

Top Headlines

Navy quickens pace for ship systems overhauls

Cyber key for TRANSCOM, being a global super power

Army commander: The service is leading the joint world in cyberspace

DARPA's 'mosaic warfare' concept turns complexity into asymmetric advantage



Videos

[[Free White Paper on Avionics Cybersecurity — Battlespace: Aloft](#)]

Section 1647 of the fiscal 2016 National Defense Authorization Act directed the Secretary of Defense to determine the vulnerability of major weapon systems to cyberattack. That review is scheduled to be complete by 2019 and its findings — though classified — will likely confirm the concerns which gave rise to it.

“There is much ‘roll up your sleeves’ work ahead of us,” admitted Dennis Miller, associate director of engineering and technical management at the Air Force’s Life Cycle Mission Center at Hanscom Air Force Base, Massachusetts. He is also director of the Air Force’s newly established Cyber Resiliency Office for Weapons Systems.

CROWS was established to manage execution of a broader effort by the Air Force to get a handle on cyber vulnerabilities stretching back to 2011. In 2015 the Air Force unveiled its Cyber Campaign Plan (CCP), which recognized the risk to the preponderance of weapons systems fielded before cybersecurity became a design-phase consideration.

The CCP looks across the acquisition, operations and infrastructure communities of the Air Force to develop a sustainable model that mitigates cyber threats and allows the service the resiliency to operate in cyber-contested environments. A Cyber Resiliency Steering Group (CRSG) made up of senior leaders from across all Air Force communities has been set up to facilitate the CCP’s goals, managing risk along with CROWS. That risk goes right to aircraft cockpits, Miller acknowledged.

1st Federal CISO offers Trump administration cyber advice

Chatting live with Gen. Gregory Touhill, the first federal CISO, on the state of federal cybersecurity and his new ventures with Cyxtera and Bay Dynamics.



Gamified AI is training next generation of cyber warriors

▶ Play Video



Wannacry investigator Marcus Hutchins arrested

▶ Play Video



Skill 08: Use Improvised Body Armor

▶ Play Video

PROTECTING

EVERY SIDE OF CYBER

[EXPLORE](#)

The Daily Brief newsletter - the top Cyber headlines every weekday morning.

EVO PDF Tools Demo

reCAPTCHA

Please upgrade to a [supported browser](#) to get a reCAPTCHA challenge.

Alternatively if you think you are getting this page in error, please check your internet connection and reload.

[Why is this happening to me?](#)

Privacy - Terms

For more newsletters click here

“The cyber threat is more than just network intrusion or traditional malware,” Miller said. “It also affects our weapon systems and presents a clear and present danger to mission assurance.”

Crossing cyber boundaries

The risk of compromised avionics goes beyond singular platforms, however. Embedded aircraft systems interact with a range of external networked systems from Link-16 and the Distributed Common Ground System (DCGS), to software update processes and systems, all the way back to the Air Force's classified secure internet protocol router email network. Compromised avionics could potentially affect broader platform-linked systems, including the F-35's ALIS to the operational flight program loaders used by a variety of aircraft. Cyber-affected avionics could pose issues for integrated air and missile defense (IAMD) systems as well.

The Air Force refers to this overlapping risk as crossing cyber boundaries. There's been little public discussion of the risk, leading to its minimization by some observers — but not all.

“There are differing opinions, but my personal view is that this is a real problem and, yes, it's a big problem,” said Neil Adams, director of the strategic systems group at Draper, a Cambridge, Massachusetts-based non-profit systems security firm.

Draper specifically focuses on embedded systems security across the military. With funding from DARPA and the Air Force, the firm has developed its own vulnerability analysis tool suites and software architectures to defend avionics.

Have certain avionics systems have already been compromised? It's a question the Air Force is reluctant to address. The Navy (NAVAIR) declined any discussion of avionics cybersecurity for this story. But, “I think it's safe to say yes,” Adams said. “There are things that have been publicly documented.”

Adams points to a 2013 Defense Science Board (DSB) report on resilient military systems, which concluded that the services could not have confidence in the ability of their cyber defense systems to thwart attacks. “That was true in 2013 and it's true today,” he said.

EVO PDF Tools Demo

Executing the plan

The 2013 DSB report broke the broader cyber threat into three categories: cyber exploits/hacking of known vulnerabilities; newly discovered vulnerabilities; and the use of full lifecycle exploits for sequenced attacks. The Air Force CCP makes similar distinctions.

Defining the scope of the problem for avionics and other systems is the work of CROWS and Avionics Vulnerability Assessment Mitigation and Protection, a program launched in 2016 by the Air Force Research Laboratory along with Ball Aerospace and SiCore Technologies. Thus far, the Air Force has identified 50 weapons systems at risk, dividing them into four priority levels.

At the top are avionics associated with the B-2, B-52H, E4-B platforms as well as satellite avionics, from Advanced Extremely High Frequency/Milstar constellations to Space-Based Infrared Systems (SBIRS) and Wideband Global SATCOM (WGS). The second tier includes avionics on the U-2 and ground-based radar (3DELRR) and detection systems (Space Fence). The third category includes most Air Force tactical and strategic aircraft, from the F-35 to the RC-135.

With maturing assessments in hand, “We know what we need to do both at the mission level and system level, we just need to execute the plan now,” Miller said.

Executing the plan will require the ability to constantly adapt. Avionics cyber threats can manifest via remote exploits (hacking) or endpoint exploits (device

interfaces). Air Force aircraft and weapons systems are not statically located; they move through threat environments as they execute missions. Different locations present different challenges but as Miller noted, modern technology has concentrated risk in unprecedented fashion.

“The reality is that as technology has evolved we have connected more and more legacy systems together and increased the potential cyber-attack surface,” he said. “The cyber threat is ambivalent to old or new systems; it’s focused on gaining access to impact the system and its mission.”

Hardening at home

The Air Force plans to combat cyber intrusion with initiatives at the operational, infrastructure and acquisition levels mentioned above. Its Cyber Squadron-Initiative establishes Pathfinder Mission Defense Teams within each major command designed to continuously map and document specific mission priorities at each wing, sharing evolving threat information and lessons learned.

Less obvious will be work done on industrial control systems issues by the Air Force headquarters’ Logistics, Engineering and Force Protection/A4 staff.

Draper’s Adams pointed out that the Air Force’s necessary reliance on a complex, distributed and often foreign network for the avionics life cycle makes the hardware, software and information assurance task especially difficult.

“All of the life-cycle phases, from R&D to acquisition, design, development, test, manufacturing and production have information that needs to be protected. It’s out there on DoD and contractor servers. New algorithms, software, hardware and designs are out there,” Adams said. “Microprocessors, micro-controllers, and memory chips are often designed state-side but the fabrication of these, including the handling of the design information is overseas. **EXOC-PDF Tools Demo** the lion’s share of electronics used in DoD systems. All of it must be protected throughout the avionics life cycle.”

The test community will likewise have to improve the way it tests and evaluates avionics systems in a cyber contested environment, Miller, the CROWS director, added. The need to do so is acknowledged by the Air Force’s own emphasis on resiliency.

Some have pointed to the Air Force’s KC-46 tanker as an example of the first weapons system to be designed with avionics cybersecurity in mind, suggesting it may be useful in roles well beyond its core tanking mission. But Miller disagreed with the idea that KC-46 represents something truly new or that it will operate in particularly novel ways.

“It’s not like we haven’t been doing anything on AF systems,” he said, citing the establishment of DoD’s Information Assurance Certification and Accreditation Process (DIACAP) in 2006, which pushed cyber-resilient design. DoD’s subsequent adoption of the National Institute of Standards and Technology (NIST) Risk Management Framework further entrenched cyber resiliency.



“This was true for the KC-46 as well as all our other systems,” Miller explained. “In addition, remember most of the KC-46 platform is a nondevelopmental military version of the Boeing 767 commercial aircraft. We have started working with DHS/FAA on commercial air vehicles; there is a lot we can leverage from each other.”

In any engagement with peer or near-peer adversaries — on even on a day-to-day footing — the Air Force and other services will have to operate with compromised systems. The CCP, AVAMP and other efforts launched by the Air Force are still young. Adams stressed that most vulnerability analysis capability in development focuses on known external threats to avionics. Draper Laboratory is concerned with the next level of embedded systems threats.


“Military systems are developed over a long period of time. The more insidious attacks are sequenced over the life cycle,” Adams said.



Comments

0 Comments

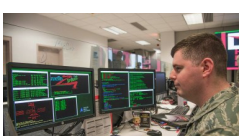
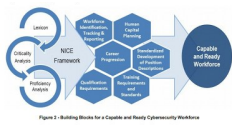
Sort by **Newest** ▼


Add a comment...
EVO PDF Tools Demo

Facebook Comments Plugin

Around the Web

Powered by Google

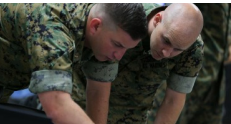


New guidelines help strengthen cybersecurity...

Cyber protection teams need more intelligence, say...

The business of national cybersecurity

East Georgia fast becoming hub for military, federal...



What's the difference between cyber and IT?

Here's how the Air Force is fighting in the cyber domain

What is the Army doing to secure and defend its cyber...

An exclusive peek inside Cyber Command's...



[Civilian](#) [DoD](#) [Congress](#) [Critical Infrastructure](#) [International](#) [Workforce](#) [Industry](#) [Thought Leadership](#)

Terms of Use

[Terms of Service](#)
[Privacy Policy](#)

Get Us

[Newsletters & Alerts](#)
[RSS Feed](#)

Contact Us

[Help & Contact Info](#)
[Advertise](#)

About Us

[About Us](#)
[Careers](#)

[MilitaryTimes](#) [AirForceTimes](#) [ArmyTimes](#) [MarineTimes](#) [NavyTimes](#) [DefenseNews](#) [FEDERALTIMES](#) [C4ISRNET](#) [FIFTH DOMAIN](#)
[HISTORYNET](#)

EVO PDF Tools Demo