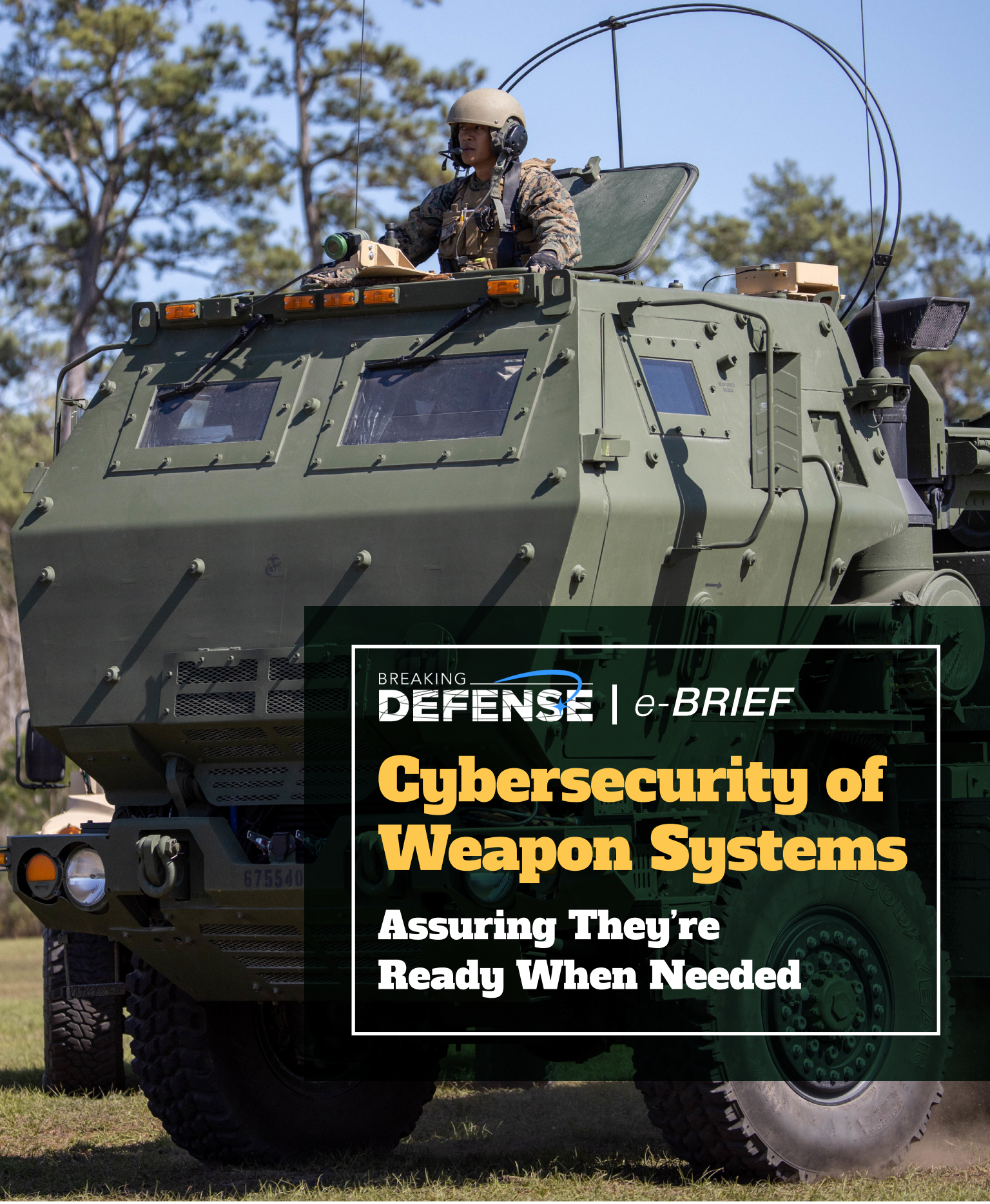


BREAKING DEFENSE | e-BRIEF

Cybersecurity of Weapon Systems

Assuring They're Ready When Needed

An editorial brief sponsored by Booz Allen®

Navy maintenance technicians conduct maintenance on the rotodome of an E-2C Hawkeye at Naval Station Guantanamo Bay.

JADC2 and Multi-Domain Operations Will Only Work If Weapon Systems Are Cyber Secure

By Barry Rosenberg, Contributing Editor
Breaking Defense, Nov. 1, 2022

For warfighters, few considerations are more important than knowing that their weapon systems, positioning, communications, and networks are fully operational for any mission.

This is an imperative for the Defense Department (DoD) but arguably is a responsibility that falls disproportionately on traditional and non-traditional companies in the supply chain that design and build those systems, provide support to tactical operations centers to monitor the security of those systems, and ensure that their software is updated and patched.

According to the Government Accountability Office (GAO), however, the DoD has struggled to ensure its weapon systems can withstand

On the cover: Marines navigate a M142 High Mobility Artillery Rocket System (HIMARS) during Exercise Rolling Thunder at Camp Lejeune, NC, in 2022.

cyberattacks. All too often, systems haven't been hardened against dynamic cyber threats and procurement contracts used to acquire the systems don't address cybersecurity requirements in the first place.

That conclusion is backed up by the Department of Defense Cyber Crime Center in the year-long Defense Industrial Base-Vulnerability Disclosure Program (DIB-VDP) pilot that concluded in April. Working with a group of ethical hackers called HackerOne, the pilot revealed that more than 400 cybersecurity vulnerabilities were found in 41 companies, as reported by Federal News Network.

DoD's management of these cyber risks is likely to improve this year as officials implement the president's recent "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" — but it will take significant effort.

It's something that needs to be addressed in order for the DoD to execute on its new concepts of operation such as Joint All-Domain Command and Control (JADC2) and multi-domain operations — both of which are network enabled, and by definition, vulnerable to cyberattack.

"These days, almost everything that we do from an Army modernization standpoint is enabled by digital transformation, on the network side and the software side," said Young Bang, principal deputy assistant secretary of the Army for Acquisition, Logistics & Technology. "To enable and ensure success in multi-domain operations, most of our systems (need to be) network enabled and connected.

"If you think about multi-domain operations, survivability is multi-domain and that includes cyber survivability, as well. When you think about newer systems (such as the HIMARS rocket system being used in Ukraine), we're trying to bake in more cyber survivability and resilience. At the same time, we're securing more of our network because some of our capabilities are platforms that are going to be enabled by our network."

The first DDG 51 Arleigh Burke-class guided missile destroyer to be built in the Flight III configuration, the future Jack H. Lucas (DDG 125), was successfully launched this past summer.

The status of weapon systems cybersecurity today

Though the Defense Department and industry would rightly agree that weapon systems cybersecurity is improving, clearly this is a long-term challenge because cyber adversaries are always researching, developing, and launching new attacks that test the personnel, processes, and technology of the DoD and industrial base. Attackers are constantly seeking to exploit known and unknown cyber vulnerabilities within traditional IT systems, special-purpose platform IT like major weapon systems, as well as legacy systems.

It's important to understand that the attack surface of any weapon platform extends to its supporting capabilities and infrastructure. This includes supply chains and logistics, maintenance systems and depots, diagnostics systems, and mission-planning systems. Together these form a system-of-systems that enable weapon platforms and all their internal components and subsystems to deliver operational effects needed for critical missions.

Further, no two platforms are the same, relatively few new ones are being developed, and most of the U.S. military's deployed weapon systems are legacy technologies that have unique obstacles to achieving greater cybersecurity and resilience.

Even though there have been various weapon system cybersecurity assessments conducted per Section 1647 of the FY16 National Defense Authorization Act (NDAA) and Section 1712 of the FY21 NDAA that tasked DoD with developing plans for regular assessment of cyber vulnerabilities in major weapon systems, reports from DoD's operational-testing directorate and the GAO continue to highlight cybersecurity shortcomings.

"The department is taking many positive steps to manage these risks," noted Gil Nolte, director of Cyber Physical and Weapon System Cyber Solutions at Booz Allen Hamilton. "For instance, the armed services developed mission-based cyber risk assessment processes. Rather than focusing on compliance regimes like the Risk Management Framework, mission-based approaches focus on identifying and mitigating cyber threats to systems or subsystems that might otherwise lead to mission failures."

That's what some might call looking at weapon systems security from a risk and threat perspective. Whether it's a weapon system or even a network that holds personally identifiable information, commonly referred to as PII, everything should be looked at as an asset and protected the same — though not necessarily protected in the same fashion.

> **'To enable and ensure success in multi-domain operations, most of our systems (need to be) network enabled and connected.'**
>
> 
>
> — Young Bang, principal deputy assistant secretary of the Army for Acquisition, Logistics & Technology

"Obviously weapon systems are critical for us to do our mission and employ our capabilities to help soldiers defend the country, and we do look at weapon systems slightly differently," said Bang. "We protect everything the same, but when we look at weapon systems, we look at it from a kill-chain perspective, or the ability to ensure that it's more resilient so that even if it's attacked or under certain threats it can still accomplish certain missions.

"From the perspective of weapon systems and PII type of data, we do protect everything extremely well. But for weapons, we actually look at resiliency and the ability to protect and execute, even if we are compromised."

Inserting Cybersecurity in the Acquisition Process

The point was made earlier that many of the concerns around cybersecurity of weapon systems arise because it was not prioritized during the procurement process. This has led to less-effective cybersecurity solutions that are bolted on at the end of the development process instead of at the beginning where they would be integral to

An F-35B Lightning II aircraft assigned to Marine Medium Tiltrotor Squadron 262 (Reinforced) executes a vertical landing aboard amphibious assault carrier USS Tripoli this past summer.

system design.

Acquisition executives now recognize the flaw in that philosophy, leading to much greater inclusion of cybersecurity requirements throughout the acquisition lifecycle. For new weapon systems, for instance, officials are setting cyber survivability requirements through the Joint Capabilities Integration and Development System (JCIDS) process established by the Joint Requirements Oversight Council (JROC).

There's even been some consideration to adding security to the list of traditional acquisition metrics alongside cost, schedule, and performance. This would make cybersecurity a matter of equal importance to those other metrics.

The military services haven't gone that far, but are making strides in setting standards for cybersecurity in requests for proposal — just as they're doing now by mandating open systems that permit the inclusion of spiral developments as the threat scenario changes over time. The Army, for example, says it will bake cybersecurity into its six major modernization priorities: long-range precision fires, next-generation combat vehicles, Future Vertical Lift, Army network, air and missile defense, and soldier lethality.

One of the Army organizations responsible for developing the defensive capabilities for those areas of modernization is the Defensive Cyber Operations (DCO) office within Program Executive Office Enterprise Information Systems (PEO EIS).

DCO is tasked with delivering defensive cyber capability in a variety of ways through a total of 10 Acquisition Category (ACAT) III and IV Programs of Record (PoR). They include: cyber analytics and detection for cyber threats; deployable and cloud-based defensive cyber solutions; rapid prototyping capabilities for rapid acquisition; Foreign Military Sales and building partner relationships; and Command, Control, Communications, Computers and Intelligence (C4I) acquisition services.

These PoRs are hardware and software capabilities employed by the Army's Cyber Protection Brigade across active duty, reserve, and the National Guard components. The brigade, in turn, provides trained Cyber Protection Teams to conduct cyberspace operations from home stations or in theater in support of Army, combatant command, DoD, and Interagency operations worldwide.

"Everybody that's been involved with acquisition from the users to the PMs themselves said the (acquisition) process is too slow," observed COL Mark Taylor, project manager for DCO at PEO EIS. "(For example) by the time we get a new helicopter out there, the threat's already two cycles past on shoulder-fired missiles and our countermeasures are not up to speed. That's even more amplified in the cyber domain where the threats move and evolve quickly in technology and in tactics and techniques.

"The traditional process where it takes two to three years to develop a requirement, (followed by) a multiyear R&D phase, and then a production phase just doesn't work in the cyber domain."

DCO's solution to speed procurement of cyber systems for the Army's modernization priorities is deliberate but much faster than the traditional way of doing things. The requirements process starts

off with a foundational document called the Defensive Cyber Operation Information Systems Initial Capabilities document. That leads to creation of an "IT box framework" where basic IT governance is established for an overarching set of requirements in areas like maneuver, detect, mission assurance, assess, plan, and conduct.

The overall document goes through the JROC and is approved at the four-star level. Accelerated cyber development begins next with establishment of a Requirement Definition Package, or RDP, each of which equates to an ACAT III or IV PoR. These active PoRs fall into areas that include forensics and malware analysis, user activity monitoring, and threat emulation.

'Everybody that's been involved with acquisition from the users to the PMs themselves said the (acquisition) process is too slow.'

— Col. Mark Taylor, project manager, Defensive Cyber Operations at PEO EIS

Steps to take to improve weapon systems cybersecurity

All weapon systems are subject to cyber threats because, for the most part, none is a stand-alone entity. Warfighting capabilities are enabled by and through a system of systems that include logistics and maintenance, supply chains, diagnostics, and mission-planning to name a few — all of which are networked enabled. These elements require robust and resilient cybersecurity. When any of these elements connect to the weapon system, they affect the cybersecurity boundary of the system and may be the gateway that malicious, unintended, or unexpected cyber vulnerabilities can be introduced.

Cybersecurity is national security — and it's fundamental for maintaining the U.S. competitive edge in the world. The U.S. must ensure its weapon systems are secure and cannot be co-opted by determined adversaries. This imperative must inform all innovation, development, deployment, and lifecycle maintenance activities for weapon systems. U.S. military superiority in conventional weapons technologies depends on having cyber-resilient weapons built using a secure supply chain, with complete awareness and minimization of foreign parts, subcomponents, materials, and software.

Any electronic device or IT component might have cyber vulnerabilities that adversaries could exploit. So it is important to look for vulnerabilities in any and all adjacent and support systems to a weapon system such as development, maintenance, training, testing, mission planning, command and control, and cybersecurity equipment. Officials need to assess these against known and potential cyber threats — and to continually monitor and reassess because known threats are constantly changing.

Here is where a capability known as digital emulation, sometimes called a digital twin, could be of great use to look for vulnerabilities and continually assess the impact of a changing threat landscape without having to perform an assessment on the actual system.

"DoD could similarly take advantage of digital twins for weapon systems and use them to continuously discover and test vulnerabilities based on threat intelligence, update cybersecurity controls, and inform risk-management decisions," said Nolte.

Achieving good cybersecurity in a weapon system development program starts with system owners, acquisition program executives, program managers, and industry partners who understand current and future cyber threats. Stakeholders should challenge their system engineers to address cybersecurity in all phases of the system lifecycle, and also hold them accountable.

They should also build-in cyber resilience to maintain critical operations if any part of the system becomes vulnerable. Finally, they should provide a means to monitor the systems to detect and respond to cyber events because, as the saying goes, if you don't monitor and measure something then you can't manage it. //

Understanding and mitigating cyber risk for DoD weapon systems is more than doable

Gil Nolte, director of Cyber Physical and Weapon System Cyber Solutions at Booz Allen Hamilton.

To help the DoD and the intelligence community strengthen cybersecurity for weapon and space systems, Booz Allen Hamilton is: 1) protecting strategic missions through threat-informed mission-based cyber risk assessments to prioritize mitigations most critical to mission success; 2) applying a deep understanding of tactics, techniques, and procedures to stay ahead of the adversary; 3) demonstrating vulnerabilities and mitigations using cyber-physical test beds, industry partnerships, and ultimately digital twins; 4) conducting cutting-edge research in resilient architectures and technologies such as Zero Trust; and 5) helping organizations achieve compliance and move to mission-based cyber risk assessments and active defense. To discuss these avenues of weapon systems cybersecurity, we talk with Gil Nolte, Director of Cyber Physical and Weapon System Cyber Solutions at Booz Allen Hamilton.

BREAKING DEFENSE: How does the president's executive order on cybersecurity attempt to address weapon systems in particular?

President Biden's May 2021 cybersecurity executive order and January 2022 memo on modernizing cybersecurity for national security, defense, and intelligence systems include some very good elements that can help enable major DoD acquisition programs to achieve near-term, fundamental improvements in weapon system cybersecurity. For example, all defense acquisition programs should aim to increase software-assurance methodologies, know and evaluate their software bills of materials, and strengthen management of supply chain risks for both software and hardware.

Anything the leadership of our nation can do to improve cybersecurity is a good thing. However, top-down directives such as this require significant resources for implementation — otherwise they can lead to unfunded requirements. And in the face of strategic competition, we must continue to prioritize cyber hardening and survivability of systems to meet National Defense Strategy requirements. The White House must ensure cybersecurity requirements are included in the president's annual budget request to Congress. And each year, it is up to Congress to appropriate adequate cybersecurity funding.

Also key is the White House and DoD's push to embrace a Zero Trust cybersecurity mindset. Zero Trust is a strategy driven by core principles: assume a breach; never trust, always verify; and allow only least-privileged access based on contextual factors. This model relentlessly questions the premise that users, devices, and network components deserve to be trusted just because they're in the network. However, when it comes to applying this approach directly to weapon systems, there are significant challenges to keep in mind.

More broadly, all DoD and private-sector organizations involved in innovation, development, deployment, and lifecycle maintenance activities should adopt Zero Trust to protect their networks and data. In our report on embracing Zero Trust for 5G, you can find a hypothetical cyberattack scenario showing how this mindset could counter attempts to steal and sabotage sensitive defense technology.

BREAKING DEFENSE: What's the low-hanging fruit that can be addressed that would lead to immediate improvements in cybersecurity?

First, non-materiel solutions like cyber training to operators and maintainers might help warfighters elevate the cyber resilience of a weapon system. This isn't just annual cybersecurity best practice annual refreshers, but training to ensure operators and

maintainers understand the cyber threat to their weapon system, how an attack could be conducted, and how they can respond.

Second, programs could benefit from performing a mission-based cyber risk assessment that would include a detailed functional thread analysis of the system's attack surface mapped to missions, system functions, and potential cyber vulnerabilities where cyber risk ratings and priority levels are determined for each point of entry into the system's cyber boundary. This could help create attack-path vignettes describing potential operationally representative cyber attacks from source to target.

These efforts aim to identify the mission-critical components and information flows in the system. This helps inform stakeholders (e.g., program executives, program managers, and industry partners) so they can prioritize their efforts to increase cybersecurity and monitoring for weapon systems, including ground-based IT support systems. Of course, this mission-based approach is a departure from traditional compliance-based reviews that solely focus, for instance, on whether a particular security control is installed and operating correctly.

BREAKING DEFENSE: What role should the private sector play in weapon system cybersecurity, and how important is it for DoD to provide better guidance on standards?

The private sector can have a huge positive role in weapon system cybersecurity — and that starts with raising standards. Across the entire weapon system life cycle, all stakeholders need to commit to managing cyber risks for these platforms through a mission lens, not simply as a compliance matter. To help bring about that culture change, industry should sponsor and participate in public "hack the machine," "hack-a-sat" or other similar events that bring crowd-sourced approaches to identify potential vulnerabilities in weapon system technologies.

In addition, industry entities can help DoD set robust standards informed by operational risks and their organizational commitments to robust cybersecurity. For instance, DoD can look to leverage private-sector investments in operational technology (OT) security testing labs such as those at Booz Allen. Our security professionals use lab environments to look across DoD, civil, and commercial sectors at platform IT/OT components — which are often shared across weapon systems and industrial control systems — for vulnerabilities and effective mitigations. We've also supported the government for decades in the development of cybersecurity standards, security control definitions, risk management framework processes, and supply chain risk management processes.

National Institute for Standards and Technology cybersecurity and privacy publications (which DoD uses) are often posted in draft for public comment prior to being finalized. This gives the private sector an invaluable opportunity to provide feedback on standards that enable cybersecurity for weapon systems.

BREAKING DEFENSE: What should be the role of mission-based threat intelligence in cybersecurity?

Threat intelligence is vital for any cybersecurity strategy. But solely focusing on today's cyber threats isn't sufficient. It's essential for defense acquisition programs to understand both the current and likely future threat environment to enable cybersecurity by design. To protect a weapon system, developers and program officials must also consider how and where the system will be used, as threats in combat abroad can be much different than threats within U.S. borders. Stakeholders need to proactively manage cyber risks and stay ahead of future threats.

Mission-based threat intelligence shows what we might know about an adversary's technical capabilities and their intent. Very rarely do those things point directly to a particular system, but a good analyst can correlate technical capability on a similar system with intent on the system being assessed. Threat intelligence should be used as a tool to focus assessments on specific areas of a system but should never be used as a filter to eliminate looking at something altogether – and understanding the criticality of a system in the context of mission operations is just as important if not more so than known adversary capabilities. Assuming a current threat profile is perfect could hand future adversaries significant opportunities to exploit unknown vulnerabilities and undermine critical missions. //

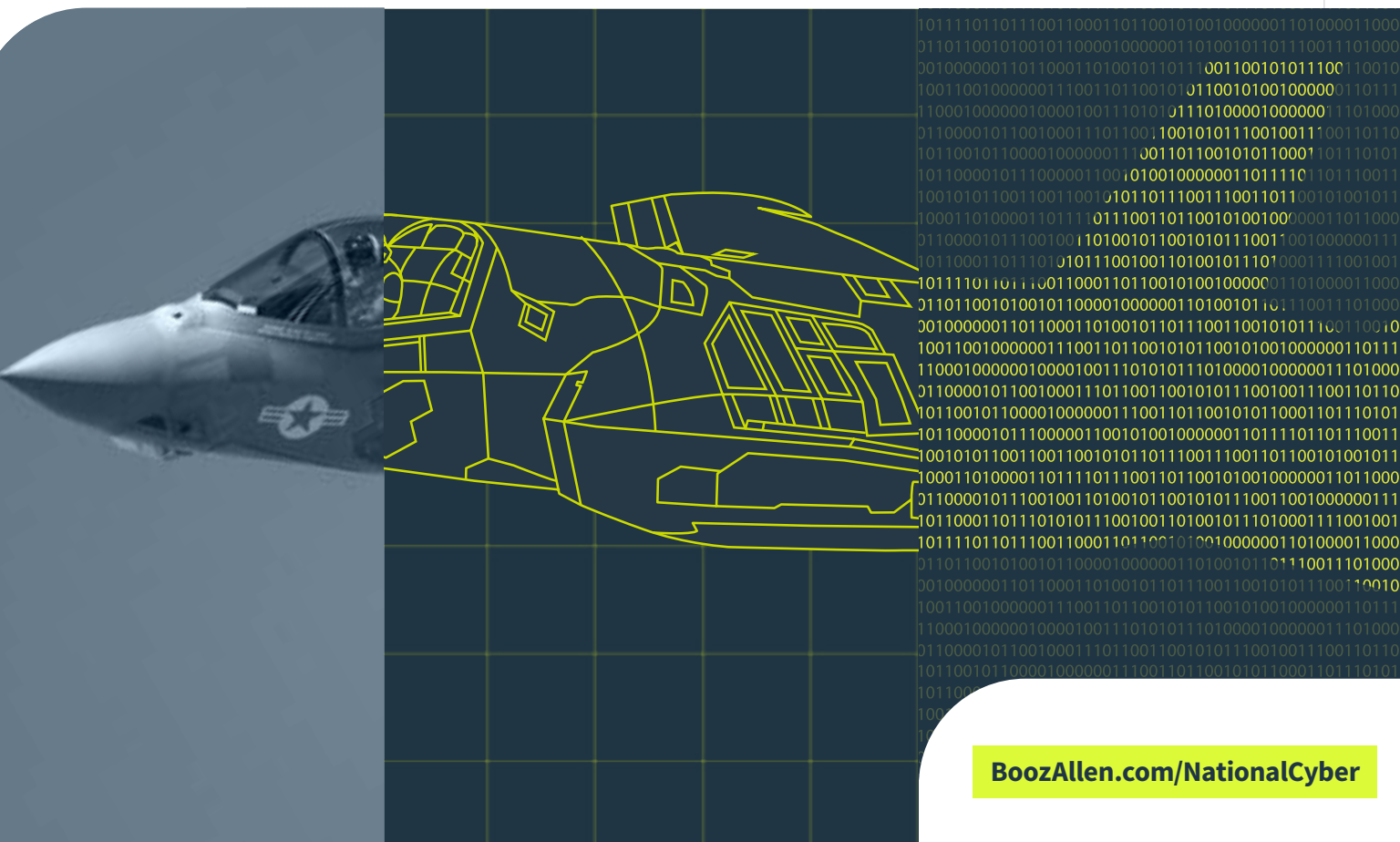
Breaking Defense thanks Booz Allen Hamilton for their support of this special brief.

Booz Allen®

THE NATION IS AT RISK.

SECURITY STARTS WITH CYBER.

The cyber landscape is increasingly interconnected. It's vast, it's complex, and it's expanding. We've brought our cyber elite onto one National Cyber team to provide cross-sector mission understanding, adversary-informed defense, and full-spectrum solutions to outpace the adversary and defend what matters most.



BoozAllen.com/NationalCyber