MANAGING CYBER RISK AND BUILDING CYBER RESILIENCE IN WEAPON SYSTEMS
MANAGING CYBER RISK AND BUILDING CYBER RESILIENCE IN WEAPON SYSTEMS

Understanding the Cyber Risks to DoD’s Weapon Systems

Two of the hallmarks that make modern U.S. military weapons so potent — their automation and connectivity — also make them vulnerable to cyberattacks. Unfortunately, these vulnerabilities continue to expand as weapon systems and their supporting systems become more integrated and interconnected. Compounding this is the unfortunate reality that the cyber capabilities of adversaries grow more sophisticated each day.

Once a weapon system is exploited by a cyberattack, the avenues for preventing that system from performing its intended function — or, worse, turning that weapon system against us — are almost limitless. Functions such as powering a system on and off, targeting a missile, navigating a ship, regulating a pilot’s oxygen levels, identifying a friend or foe, and flying an aircraft are typically enabled by software and therefore potentially susceptible to compromise. Much of the software that carries out these weapon system’s functions was never designed with cybersecurity in mind — and, even if it was, it was often not designed to anticipate many of the advanced cyberattack methods in use today.

Department of Defense (DoD) organizations understand very well that these vulnerabilities pose significant threats to military readiness. In response, DoD is actively developing strategies and programs that address the cyber risk inherent in weapon systems and the non-traditional IT that support these systems. Responding to recent congressional and leadership directives — most notably, the FY 2016 National Defense Authorization Act’s section 1647 — defense organizations are taking inventory of and assessing vulnerabilities throughout their weapon systems arsenals.

This is an incredibly complex undertaking. Many weapon systems functions are carried out by complex systems comprised of control systems and embedded IT. These systems and technologies are comprised of components, architectures, interfaces, and protocols with unique cybersecurity challenges from traditional IT. These systems include the embedded components that translate data and sensor information into precise mechanical movements that fly an aircraft or unmanned aerial system or steer a ship.
Thinking Differently About Cybersecurity for Weapon Systems

Because weapon systems rely on different architectures, interfaces, and protocols than do traditional IT systems, it can be challenging to apply traditional cybersecurity tools and approaches to protect, monitor, and assess the cyber risk associated with major weapon systems. This means the department must think about the challenge of securing them in a different light than it has traditionally treated IT cyber risk.

First, the cybersecurity of weapon systems needs to be treated as a function of operational and mission readiness. Weapon systems owners and operational commanders need to understand the cyber risk their system is carrying, and its impact on mission success. This requires an in-depth understanding of both the adversary threat landscape, as well as the security architecture of the system, including end components and sensors as well as critical dependencies and potential vulnerabilities. Organizations need to use a combination of system security engineering discipline, application of a viable risk management framework, cybersecurity testing (e.g., blue, red teams) and wargaming to better understand cybersecurity system risk posture.

DoD must also address the cybersecurity of weapon systems in a mission context. Technical experts cannot solve the problem without understanding the underlying mission requirements. Without balance in this activity, the effectiveness of the weapon system will be negatively impacted.

Perhaps most challenging, they must address the reality that the cyberattack surface for weapon systems is vast and complex, extending well beyond weapon systems and subsystems to include the many ancillary systems they connect to. These include maintenance and diagnostics, communications, data links, command and control, and other critical support systems. Understanding how these myriad systems interface with each other to pose vulnerabilities, and then assessing and prioritizing those vulnerabilities in specific terms, is a monumental challenge. Creating a comprehensive inventory of all these assets is tedious and time-consuming, but is absolutely essential to create a viable risk management program.

Another area of concern relates to the cyberattack surface, since cyber effects are not limited to systems with IP addresses. DoD is focusing on building capabilities to explore other avenues of attack including:

- **Radio Frequency Manipulation** — Either using an RF signal to create a cyber effect or vice versa. This is different than EW testing in that the effect is not necessarily jamming or physical disruption. Instead, it could involve taking advantage of faulty logic programming, bandwidth issues or use of unneeded functionality.

- **Supply Chain Risk** — Manipulation of hardware and software to enable sabotage or subversion of critical mission functions.

- **Attachments** — A weapon system might be totally resilient for its own mission until someone attaches something new to it.

Only an integrated security approach will help create a more resilient platform. Because weapon systems are so central to military readiness and efficacy, it is not enough to simply bolt on security features to a weapon system or subsystem and then monitor it. Each must be carefully assessed to understand which component functions are vital to support critical mission tasks, so they can be enhanced to possess greater resiliency in cyber-contested environments. Embracing these principles will create a system much more resilient to attacks.
GAINING SHARP VISIBILITY INTO THE CYBER RISK POSTURE OF WEAPON SYSTEMS WITHIN THE CONTEXT OF MISSION EXECUTION CALLS FOR AN APPROACH THAT BUILDS UPON ESTABLISHED METHODS OF MANAGING CYBER RISK BUT ADDS AN INTEGRATED, ENGINEERING AND ARCHITECTURE-BASED OVERLAY THAT BUILDS CYBER RESILIENCE.
Fortunately, it is possible to untangle the complexity, and gain sharp visibility into the cyber risk posture of weapon systems within the context of mission execution. Doing so calls for an approach that builds upon established methods of managing cyber risk but adds an integrated, engineering and architecture-based overlay that builds cyber resilience.

**ADVANCED ANALYTICS HELPING CYBER RISK MANAGEMENT IN WEAPON SYSTEMS**

Several frameworks have been created and proliferated across the Federal Government to implement cybersecurity and manage risk. These frameworks address implementation of cybersecurity for weapon systems and are essential parts of a system-based security effort. However, these frameworks are not always applied consistently, and there is a general lack of available tailored guidance specific to weapon systems.

Moreover, an effective cybersecurity program should extend further than merely implementing a mandated framework. The impact of this collective set of actions should be analyzed with respect to the overall operational effectiveness of the weapon system. Without analytically derived insight to understand connections both within and external to the platform, an accurate risk assessment cannot be made. This does not reflect any deficiency in the risk management process itself, but rather arises from the frustratingly opaque interconnections of components within the weapons platform.

The lack of visibility has other cascading effects — for example, it makes it difficult for cyber risk managers and weapons operations teams to align their scanning and other tools, when compatible, with mission objectives. Those tools already tend to reside in isolated silos, due in large part to the current acquisition process — different organizations purchase their own tools, usually for specific applications. As a result, cyber risk managers and weapons operations teams may not be relying on the same data and can end up working at cross purposes.

The key to addressing this is taking advantage of advanced analytics in a thoughtful way. Applied correctly, advanced analytics can provide insights into the entire attack surface of weapon systems and their supporting infrastructures. In addition, the analysis provides further depth to the critical functions of the traditional cybersecurity lifecycle.

**BUILDING CYBER RESILIENCE IN WEAPON SYSTEMS**

To achieve the objectives established in Section 1647 of the NDAA requires a commitment to the philosophy of building resilience — the capacity of systems to withstand disruption and continue operating with minimal impact on output or function.

While risk management looks at how to assess, prioritize, and mitigate vulnerabilities and risk to the system, resilience looks at the operational elements of the weapon system and assumes that some disruptions will succeed, and some operational effectiveness will be impacted. Understanding that weapon systems are comprised of many operational components that may operate independently and relatively autonomously, resilient design identifies weaknesses that exist within the network structure and leverages its strengths to compensate.

One of the biggest strengths enabling resilient design is the interconnectedness of the non-traditional IT system components within a weapon system and their ability to provide needed functionality in the event other nodes are disabled. So, while there may be many paths to vulnerability and many ways to fail, there are also multiple ways for the system to quickly heal itself to achieve functionality.

The term resilience comes from the Latin word “resiliere” which means to jump back. In our usage, it is probably more accurate to frame the meaning as bouncing back but the idea is the same. This is
the core concept of cyber resilience, as
demonstrated in the figure below.

Cyber mission resiliency is being able to continue to 
execute the assigned mission even in the face of a 
cyberattack. This could be through redundant 
components or changes to TTPs. For example, if a 
particular subsystem on a ship starts acting 
strangely, the commander might simply switch it off. 
The ship may lose a degree of functionality or the 
mission might take longer to complete, but the 
mission will go on.

It could also mean totally swapping out one system 
for another. For example, if it’s known that the F-16 
is vulnerable to a particular type of cyberattack when 
going against a particular adversary, USAF might 
use the F-22 instead. In this case the F-16 would not 
be cyber resilient, but the mission would be. DoD 
operational components can build resilience by 
balancing two approaches:

- Architecting weapon systems to ensure the 
highest level of mission effectiveness after a 
cyberattack through redundancies, backups and 
fail-safes.
- Designing rapid responses to return a system or 
network to operating capacity as quickly as 
possible.

The decision regarding which of these approaches 
should be applied to a given weapon system to 
achieve the optimum performance, while also 
managing risk and minimizing susceptibility to 
downtime, is challenging and requires the insight 
gathered through the analytics in the risk 
management process.

**Putting It All Together**

Making all of this work requires more than the 
application of mandated risk management 
frameworks and expertise in advanced analytics. It 
also requires deep experience and expertise with 
military missions. Mission understanding is critical 
to ensuring that the many subsystems and external 
connecting systems of a weapon system are 
effectively mapped to their mission-essential tasks. 
Vulnerabilities must be appropriately assessed and 
prioritized in the context of those critical missions. 
And the right functions and capabilities must be 
infused with appropriate levels of resilience, so the 
weapon system’s effectiveness is assured in 
degraded environments. In short, it is this mission 
understanding that helps ensure that focus and 
resources are directed effectively and efficiently to 
assure mission readiness.

By employing this type of dynamic cyber risk 
management program for weapon systems, driven 
by advanced analytics and sharply focused on 
mission execution, DoD organizations can fully 
understand, monitor, and mitigate their weapon 
systems cyber vulnerabilities and system risks and 
set the conditions to build overall mission resilience.

---

**Resilient Response** — The impact of the 
event on the operational effectiveness of the 
weapon system is reduced in terms of both 
degree of impact and time to recover through 
a combination of better system design and 
Improved response time/decision making

**Non-Resilient Response** — The 
threat event negatively impacts the 
operational effectiveness of the weapon 
system in terms of degree of impact and 
time to recover
OUR AUTHORS

For more information please contact our experts:

David Forbes
Principal
Forbes_David@bah.com

Jandria Alexander
Principal
Alexander_Jandria@bah.com

Kyle Miller
Chief Technologist
Miller_Kyle@bah.com
About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.