Resilience in the Face of Cyberattacks: Cyber Resilience Guidance for Military Systems

Chuck Crossett

ABSTRACT

Military systems must perform their missions under threat and during extreme conditions. This required resilience is paramount to our warfighting ability and national security. Ensuring that our systems are resilient in the face of cyberattacks is a challenging task. This article proposes 10 principles that should be considered by the operational forces and system acquisition offices that are essential to making sure military systems are able to perform their missions in the face of this threat. These principles derive from the basic premise that to be truly resilient, the system (1) must make it as difficult as possible for the adversary to access and traverse to its target, and (2) must have measures in place to continue its mission regardless of whether the adversary is able to attack. U.S. military systems cannot assume that an adversary will not succeed, and therefore the mission must be resilient to the attack's effect.

INTRODUCTION

The subject of resilience within this article is more confined than elsewhere in this issue of the *Johns Hopkins APL Technical Digest*. It deals only with resilience under a certain kind of attack—one against the system via its information storage, processing, and communication components through digital means. This is commonly referred to as a cyberattack, and that term will be used throughout this article. However, the discussion cannot be confined to only information and communication systems. The military mission must be able to be accomplished in the face of a cyberattack on the system, and sometimes this may include non-cyber systems or actions.[1]

Cyberattacks are often assumed to have one or more of three effects—effects on the availability, integrity, or confidentiality of the system. (In most definitions of cybersecurity, the primary objective is to protect the confidentiality, integrity, and availability, or CIA, of information within a system.[2] While there are debates about expanding the definition beyond just protection of information,[3] the CIA triad is still frequently used to foundationally explain the need for this security.) Availability attacks are meant to restrict or deny access to particular data or nodes of the system. Denial-of-service attacks and ransomware are examples of availability attacks. Integrity attacks modify the data so that the system operates in a way that is advantageous to the attacker. Modification of records or changes to a sensor's reading before it is received by a controller are examples. Confidentiality attacks are breaches of trust or secrecy. They disclose data, such as a password, to others.

Attacks with any of these three outcomes may have secondary effects beyond the boundaries of the targeted system. A changed sensor reading can mislead a controller to determine that a heating element needs to be activated, causing the system to overheat and sustain physical damage. Attacks can be delivered (whole or in part) outside of the targeted system proper as well, whether via a human clicking on a malicious e-mail attachment, some electromagnetic means of interfering with the system's operations, or a backdoor implanted at the factory where components are manufactured. Responses to the attack may also be best handled outside the cyber domain. Since mission resilience is paramount, other means of achieving the mission, such as physically enacted operations or out-of-band parallel systems, must be considered and used.

A HOLISTIC APPROACH TO RESILIENCE AGAINST CYBERATTACK FOR MILITARY SYSTEMS

Two foundational strategies underlie our recommendations for maximizing resilience: increase the cost for the adversary to attempt and accomplish an attack and decrease the impact of attacks as much as possible. (Adversary cost includes not only the resources to develop and enact the attack but also the effort required to ensure the attack works. Therefore, difficulty to access, traverse, execute, and maintain the attack is all part of the adversary's "cost" that we are trying to maximize.) Resilience is necessary because risk cannot be eliminated. Since military systems must last years (in some cases even decades) and face the world's toughest foes, the U.S. military simply cannot assume that the adversary will not succeed.

Our mind-set, then, must become one of making an attack as expensive and as difficult as possible to accomplish. And even if the cost of an attack can be dramatically increased, we should still assume that the attacks will occasionally still be effective, often in unforeseen ways. Therefore, true resilience means our military systems have to perform throughout an attack, warding off the attack as much as possible at a reduced capacity, transferring the mission to other components/systems, or having alternative means of accomplishing the mission.

This article posits 10 recommendations for a military system to be resilient to a cyberattack. Most apply to systems being used today, to be incorporated into current operations and maintenance. Others apply strictly to new systems, to be incorporated during the conception, design, acquisition, and installation of new devices, systems, or even whole military platforms. The most effective resilience action a program office can take is to engineer resilience into the system from the start, but we cannot ignore the systems that are vulnerable during today's operations. (Also consider that mission resilience may need to span program offices or even operational commands. The nuclear triad provides a good example of how a mission can be resilient against various threats even if one type of system is vulnerable.) The United States has to do all it can to protect and defend the legacy mission equipment and capabilities until more secure systems are available.

CYBER RESILIENCE GUIDANCE FOR MILITARY SYSTEMS

1. Design to a cyber adversary like you design to a kinetic one.
2. Design out vulnerabilities as much as possible.
3. Increase the cost for the adversary to get into your system.
4. Increase the cost for the adversary to get around inside your system.
5. Know what is going on in the system at all times.
6. Decrease the impact of the attack.
7. Include recovery and reconstitution of the system in your resilience scheme.
8. Assess and test constantly.
9. Protect the system as you build it.
10. Protect the system as you operate and maintain it.

These cyber resilience principles are consistent with other proposed tenets and guidelines, for example those described in Refs. 4–6. The purpose of this article is to stress the need for each particular recommendation, as well as make the case that they must be considered part of the holistic system trade space, both during design and during mission planning and operations. Most of the recommendations involve either the design of the system itself, ways the system's resilience can be improved while it is under operation, or principles to enact while acquiring new systems as part of the acquisition process. Therefore, the rest of this article is divided into those three areas.

Technical Design Recommendations

The proposed principles impact different segments of the technical design, which overlap to some degree. There are recommendations for limiting access points

to make it harder for attackers to gain entry into your system. They will sometimes still find a way in, but there are many ways to make the terrain (the paths from access point to target) difficult for them and advantageous for you in terms of situational awareness and defense. By assuming attackers will get through your defenses and accomplish their attack no matter how difficult the cyber terrain, you can take steps to lessen the attack's impact on your mission. The idea is to enable the system to continue to perform the mission as much as possible during and after the adversary takes action.

Consider designed-in resilience against cyberattack in the same manner as you would consider resilience against any other threat, be it kinetic, environmental, nuclear, or electronic. Since cyberattack is not currently a well-understood threat vector for our assessment and design of systems, DoD is still working through how to account for it in the design, integration, testing, and operational environments already established. Cyber needs to become one of the design-to threats for a system in the near term. The hope is that this article provokes that installation into the normal systems engineering cycle.

For new systems to counter an adversary's access, terrain, and impact, the key is robust and resilient design of the system from the ground up. And that means designing out as many vulnerabilities as possible. Extensive use of COTS software and hardware in current systems has proven to be an advantage to the cyberattacker. Known flaws in design and available exploits for those vulnerabilities make the use of COTS elements a challenge for cybersecurity. For new systems, COTS components must be tailored, constrained, and carefully considered because of the risks. Removing or inhibiting all functionality that is not strictly necessary for your mission is a key step. Thorough testing and verification of all COTS elements for vulnerabilities is also recommended, as is designing a scheme to quickly patch all discovered vulnerabilities throughout the life cycle of the system. It is too expensive and risky to apply those considerations after the design is complete. For existing systems, keeping up to date with patches and updates is a difficult task (mostly because of reaccreditation, limited connectivity in time and volume, or both), but doing so is really the minimum possible measure for our systems. It can only be the first step.

If your system will be custom designed, use all available techniques (e.g., formal methods or other methods of software assurance)[7] to ensure that it will do what it is intended to do for the mission, and nothing more. Simplifying software and hardware designs will allow for easier verification and validation of the system's security, as well as enable easier characterization and prediction of failure modes when an attacker does hit.

Of course, it is impossible to develop a system that has no vulnerabilities lurking inside. Therefore, you must limit the accessibility of the system to make it as difficult as possible for an attacker to gain entry. Rigorously explore all possible access points of your design or existing system, and give those nodes extra protections and sensing. All systems will have some means of access, and awareness of and close monitoring of those points will make it more difficult for the adversary to exploit them.

Remember that the operator uses these access points as well and can misuse the system intentionally or not. To the extent possible without inhibiting the mission, verify all inputs, all accesses, and all activity. Log everything. And do not forget that maintenance systems may have access to your system as well. These are often outside of the normal design specifications (and security requirements) of the military system, so you must either incorporate extra security into the entire maintenance system or design boundary protections, input checking, and access verifications and log all data for these as well.

But even the best boundary protections cannot be assumed to keep all attackers at bay (refer to warfare history textbooks and the Maginot Line). The advanced adversary will be able to find a way inside, and therefore, to be as resilient as necessary, the defenses inside the system must be as strong as the boundary. There are many different schemes and techniques for making the cyber terrain more difficult for an attacker to traverse, and the choices will depend on your system and its mission, performance needs, and scale.[8]

Recalling the foundational recommendation to increase the adversary's cost of attack, diversification of all sorts (e.g., different operating systems and different vendors for hardware) is highly recommended so that movement inside your system is difficult (requiring a number of exploits) and increases the adversary's research, development, and reconnaissance costs. Note that this suggestion conflicts with our former recommendation to reduce complexity. Obviously, this trade between two solutions must be analyzed and deliberately balanced, since they will work against each other. There is no recommended blend that is generalizable for all military systems. Here, deception and moving-target defenses will pay off if incorporated. They lower the adversary's knowledge of how to attack efficiently, which can lower the adversary's probability of accomplishing their goal.

Also highly encouraged is the segmentation of mission functionality and/or areas of trust within the system. It is likely that some components must have complete trust in each other's output, while some components operate at a lower level of trust. The components requiring complete trust should be separated and better monitored at their interfaces. Beware of the common backbones, which provide easy ways for an adversary to move at will.

The last main recommendation is to design in ways that enable the system to accomplish the mission regard-

less of the attack. Redundant and diverse paths for mission functionality decrease the chances that one attack can be accomplished against all paths simultaneously. Recovery of components to a known, good state should also be part of the design, if possible as part of the mission timeline. This is an area where virtualization of components may have distinct advantages when high availability is required. We would also highly encourage exploration of reconstitution approaches, where gold-standard spares are quickly available or redundant systems can be quickly incorporated to perform the mission when another is attacked. Certainly, these options all depend on the situation and context of the operational requirements, but incorporating them into the trade space may show highly efficient and secure alternatives to building a super-hardened system.

Cyber Resilience During Operations

Resilience while operating the system should also be a major consideration during the design process for new or reengineered systems and components. This section discusses factors for improving resilience and maintaining assurance in the system while it is in operation.

Part of the current difficultly in understanding how to modify operations for resilience is our lack of detailed understanding of our systems as they are in use. It is critical to gain cyber situational awareness capabilities across our systems and networks as much as possible. Knowledge that the system is under attack is as important as protecting from the attack itself, since some attacks will always get through the defended perimeters.

Striking the balance between monitoring your system at a detailed level and knowing how to interpret the data is a technological issue at the moment but one that is quickly improving. Making sense of the volume of data available and determining what it all means is not a subject of this article, but it is a vital step. The more that the system/operator can tell when something is amiss, whether it is malicious, and how it may affect mission performance, the larger the advantage for the defender. Identifying whether defensive actions can be determined onboard or elsewhere, and whether preplanned or dynamically determined, should be part of a larger operational resilience scheme that likely involves multiple systems or platforms.

Cyber hygiene procedures should be implemented to ensure that "back-to-gold" states are achieved, and that cybersecurity is part of the regular maintenance of your systems under operation. For very critical missions, we recommend a continuous assessment program, where the health and status of systems are regularly (and randomly) checked, and systems are assured to be trustworthy and tested for known behavior. Since cyberattacks may involve prepositioned malware, accesses, or data changes (think of phishing attacks, where access is gained through e-mails), one cannot assume that the system continues to be safe once it starts operations, even if it is away from all proximate adversaries.

Certainly, non-mission systems (such as maintenance laptops), health and status reporting communications, and quality-of-life systems, and even nondeliberate changes to make operations easier once in the field/at sea/in flight must be viewed as offering potential ways for an adversary to get into and around a very well-designed system.

Once the technology is available to enable awareness of the cyber situation and procedures are in place to secure the system during operations, operators must be prepared for and knowledgeable on what to do when indications and warning tell them that something is wrong and they are under attack. Operational procedures have to be established or rewritten to accommodate this new threat. If a computer goes down, rebooting it during crucial mission operations may not be the best option. Ready backup systems for vital functionality, strictly physical procedures, or completely isolated nonidentical means may need to be available. Training for these circumstances must be incorporated as cyber becomes an integrated domain of warfighting.

Acquisition Principles for Cyber Resiliency

Whereas technical design principles were discussed earlier, this section emphasizes the importance of security within the acquisition process, beyond design. The first principle is likely obvious from the technical design recommendations above. Cyberattacks should be considered a threat vector in much the same way a kinetic threat is. For some military systems, this means that cyberattack scenarios must be part of the mission scenarios used for operational performance requirements. For others, it may be necessary to incorporate cyberattacks as part of the operational availability requirements or other key parameters. What is encouraged in any case is consideration of the cyber threat from the very beginning of analyses and trades and a traceable flow through the requirements to each component.

Design and operational testing should also incorporate cyberattacks as mandatory elements, both at the component and integrated system levels. Testing beyond the specifications is highly encouraged, since failure under cyberattacks is currently not well studied or understood for most systems, and knowing how the system will fail is as important (or more important) for resilient design as knowing the chance for failure.

Processes and security procedures for manufacturing, transporting parts, and warehousing should also be designed with cybersecurity in mind. The supply chain is an attractive target for advanced adversaries because it can be much simpler for them to attack at a time of their choosing. Supply chain risk management,

diversity of parts, and security of transportation and storage will all increase the costs and effort required of an attacker.

Last, but certainly not least, the technical specifications (and those of operations) of a military component are a treasure trove for an adversary. Since military systems are tightly regulated in terms of their design, their variation, and their conditions or operation, knowing exactly what their attack path will be, what the system has (and does not have) in terms of protections, and how the warfighters will interpret any fault or error makes designing an attack plan much simpler (and cost effective). Protecting the system as you build it, ensuring that specs, plans, and manuals are not easily obtained or purchased, can go a long way to making attackers' jobs harder before they even begin.

CYBER RESILIENCE GUIDANCE FOR MILITARY SYSTEMS

1. **Design to a cyber adversary like you design to a kinetic one.** Consider cyberattacks a design-to threat. Refuse to be the weak link since the mission will be at risk if even one system has vulnerabilities and does not have strong cybersecurity. Do not ask for exemptions. Understand the risk and know what data/components are absolutely critical to the mission. You will not be able to protect everything equally. Assume that the adversaries are leaning forward. The payload may not be delivered immediately before the attack. It will likely already be planted and waiting.

2. **Design out vulnerabilities as much as possible.** Reduce complexity and functionality across the architecture. If you incorporate commercial products, legacy elements, or open-source code, remove or prohibit everything not strictly needed for the mission. If you build your own code, validate that it only does what you mean it to do.

3. **Increase the cost for the adversary to get into your system.** Make it as difficult as possible for an adversary to gain access. Assess all possible entry points used in day-to-day operations, including maintenance systems. Ensure all users are authenticated and well trained on the risks to the system. Implement as many second-checks as you can to reduce the risk from an insider who has access to the vital areas of your system.

4. **Increase the cost for the adversary to get around inside your system.** Make it hard to traverse. Build in choke points and monitor them. Use diverse software and hardware and segment areas that are higher priority to protect. Virtualize, randomize, and encrypt what is necessary to protect the mission.

5. **Know what is going on in the system at all times.** Have sensors across your system. Have situational awareness of health and status, of behavior, and of users. Have analytics that know the difference between normal, anomalous, and malicious behavior, and have preplanned actions for operators to enact when something is wrong.

6. **Decrease the impact of the attack.** Have redundant data paths, especially along diverse hardware/software suites, and separate functionality within your system. Have backups for critical mission capabilities, including out-of-band or non-cyber means for the most important mission functions.

7. **Include recovery and reconstitution of the system in your resilience scheme.** The quicker you can get the system back into a known and trustworthy state, the faster you can continue your mission. Design your system to preserve state so that you can restart as soon as possible.

8. **Assess and test constantly.** The cyber situation is not static. The adversary's capabilities are constantly improving, and you must stay informed of their abilities. Insiders (witting and unwitting) constantly pose a risk to the system. Welcome red teams to repeatedly test your system and inspect everything deeply.

9. **Protect the system as you build it.** Cyberattacks can start within the acquisition cycle. It is far too easy for an adversary to develop an attack when they know the system's design as well as you do, so protect the plans. The supply chain often has the weakest security, so be sure to inspect, validate, and secure the factories/developers. Use deception and obfuscation where possible.

10. **Protect the system as you operate and maintain it.** Do not treat cybersecurity like a checklist or something to be bolted on for protection. Updates, patches, reboots, and other hygiene measures have to be a normal part of operations of the system, as do training, testing, and drills related to cyber events. Have operational tactics ready when an attack occurs, just like you would for a kinetic attack.

CONCLUSION

This is a rather broad overview of recommendations, and how to incorporate them for a specific military system requires far more detail than can be described here. The recommendations are meant to be motivators for a holistic thought process across existing and new systems, from design to operations.

Mostly, they are meant to emphasize that being resilient against adversaries that will use cyberattacks either as a goal of itself or as part of a larger strategy requires us to think across all these avenues. The ultimate goal is to give adversaries as small a chance as possible to attack our systems and succeed. Again, to increase the costs and effort for the adversary to use this route, and to decrease an attack's impact on the success of our mission, is our current goal. Implementing these ideas at least in part will help us achieve this goal.

ACKNOWLEDGMENTS: The author thanks the many reviewers of this work, including Rick Alfini, Scott Casper, Peter Dinsmore, Shaun Hutton, Sean Manning, Michele Midgley, Rob Nichols, and Troy Osten. He is also indebted to the many people whose concepts and ideas have provided the basis for these recommendations, because none are original to this work but have proven (so far) to be current best practices. Special thanks also to Jim Gosler and Sue Lee for their framing of these concepts during internal discussions and briefings.

REFERENCES

[1]Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, Office of the USD for AT&L, Department of Defense, Washington, DC (Jan 2013).

[2]"ISO/IEC 27002:2013 Information Technology — Security Techniques — Code of Practice for Information Security Controls," https://www.iso.org/standard/54533.html.

[3]von Solms, R., and van Niekerk, J., "From Information Security to Cyber Security," *Comp. Secur.* **38**, 97–102, doi.org/10.1016/j.cose.2013.04.004 (Oct 2013).

[4]Bodeau, D., and Graubart, R., *Cyber Resiliency Design Principles*, MITRE Technical Report MTR170001, MITRE, Bedford, MA (Jan 2017).

[5]Director, Operational Test & Evaluation, "FY16 Cybersecurity," in *FY 2016 Annual Report*, Office of the Secretary of Defense, Washington, DC, pp. 441–450, http://www.dote.osd.mil/pub/reports/fy2016/pdf/other/2016cybersecurity.pdf (Dec 2016).

[6]Department of Defense, *Cybersecurity Test and Evaluation Guidebook*, version 2.0, Department of Defense, Washington, DC, https://www.acq.osd.mil/dte-trmc/docs/CSTE%20Guidebook%202.0_FINAL%20(25APR2018).pdf (25 Apr 2018).

[7]Pendergrass, J. A., Lee, S. C., and McDonell, C. D., "Theory and Practice of Mechanized Software Analysis," *Johns Hopkins APL Tech. Dig.* **32**(2), 499–508 (2013).

[8]Pecharich, J., Viswanathan, A., Stathatos, S., Wright, B., and Tan, K., "Mission-Centric Cyber Security Assessment of Critical Systems," in *Proc. AIAA Space Forum*, Long Beach, CA, pp. 1–23, doi.org/10.2514/6.2016-5603 (2016).

Chuck Crossett, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Chuck Crossett is a member of the Principal Professional Staff in APL's Asymmetric Operations Sector, where he serves as chief scientist and section supervisor within the Resilient Military Systems Group and as acting chief scientist for the Cyber Operations Branch. He has over 25 years of experience in leading the development of models and simulations of systems and analyzing new missile and cyber systems. He previously taught for the Engineering for Professionals program at the Johns Hopkins University Whiting School of Engineering and is a historian specializing in early systems sciences and computer modeling. His e-mail address is chuck.crossett@jhuapl.edu.