The State of Cyber Resilience: Now and in the Future

Thomas H. Llansó, Daniel A. Hedgecock, and J. Aaron Pendergrass

ABSTRACT

The Department of Defense has dealt with a multiplicity of threats throughout its history, including espionage and insider threats, as well as chemical, biological, radiological, nuclear, and explosive threats. As the department has increasingly incorporated cyber components into weapons and supporting systems in recent decades, threats from cyberattack have taken their place alongside these existing threats. At the same time, traditional cyber defenses designed to keep cyber invaders out of our systems have not always proven effective. This article discusses cyber resilience as a means for helping to ensure mission survivability despite adverse events in cyber. The article covers the state of cyber today, why cyber can be so vulnerable, and how resilience techniques can complement traditional cyber defenses to help ensure the larger mission. The article concludes with a discussion of cyber and cyber resilience in the future.

INTRODUCTION

Cyber resilience is an idea increasingly viewed as vital as society becomes ever-more dependent on computer-enabled "cyber" systems. This article begins by summarizing the nature of today's cyber systems and why they remain so difficult to fully secure. This discussion motivates the next section, which elaborates on the idea of cyber resilience, including a working definition of cyber resilience, an exploration of how cyber resilience ties to the mission/organizational level, and a brief sampling of resilience frameworks, mechanisms, and quantification approaches. Finally, the article speculates on the future of cyber resilience. Along the way, the article describes ongoing cyber resilience work at APL, including the Cyber-Resilient Ship envisioned future initiative, which focuses on future Naval platforms that can operate through and recover from cyberattacks despite reliance on compromised components. (See the article by Gregg, Nichols, and Blackert, in this issue, for more on envisioned futures initiatives.)

CURRENT STATE OF CYBER

In 2021, cyber is ubiquitous, supporting a broad range of applications, such as banking, entertainment, home security, voting, and weapon systems. Of course, the use of cyber has its downsides. We are all familiar with the specter of identity theft and online fraud, but cyberattacks can also have potentially life-threatening consequences in contexts as varied as medical infusion pumps, self-driving vehicles, and critical infrastructure.

Meanwhile, in cybersecurity circles it has become nearly axiomatic that despite more than two decades of effort, the community is unable to fully secure cyber-intensive systems.[1] It is generally safe to assume that determined adversaries will eventually penetrate high-value systems, or are already inside via malicious implants embedded in supply chain components.[2]

Why are cyber systems so hard to secure? In short: assurance, complexity, and connectivity.[3] The trustworthiness of modern cyber systems is often impossible to verify. Most large-scale cyber systems are not constructed from rigorous specifications, and they tend to be composed of ever-more intricate layers of functionality that incorporate third-party libraries and open-source elements, many of uncertain pedigree. The interconnected nature of cyber systems is a further complicating factor, as every additional direct or indirect connection represents a potential attack vector.

The use of mathematically rigorous techniques, known as formal methods, to specify and validate cyber functionality can help, as can the use of various trusted computing approaches, though scalability issues persist.[4–6] (See the article by Kouskoulas et al., in this issue, for details on some of the work APL is doing in formal methods.) Assured technology is not enough, however; people and processes are also critical. People can be relatively easy to fool,[7,8] and business/mission processes may not anticipate all the different ways in which supporting cyber systems can fail. Vulnerabilities introduced during design and integration remain a major challenge, with even the largest vendors and user organizations deploying expensive “bug bounty” programs to aid in the search for flaws.[9,10] Indeed, research suggests that a majority of software vulnerabilities remain latent in large-scale systems, awaiting discovery by attackers and defenders.[11,12] At the same time, advances in the fundamental science of cybersecurity lag as attention and energy is focused on other areas, such as creating and conforming to resource-intensive compliance programs[13,14] whose effectiveness is difficult to ascertain.

In summary, the cyber community struggles to completely secure complex cyber systems, with attackers maintaining an asymmetric advantage over defenders. Nonetheless, organizations must still achieve their business/mission functions despite growing dangers associated with their dependence on cyber. In fact, what ultimately matters to organizational stakeholders is that those functions remain robust in the face of cyber threats—that is, that they are resilient.

CYBER RESILIENCE

While interest in cyber resilience has grown significantly over the last 10 years, resilience itself is not a new concept. Examples of non-cyber resilience mechanisms include use of backup generators in hospitals and municipal flood control tools such as diversion canals and storm water basins.

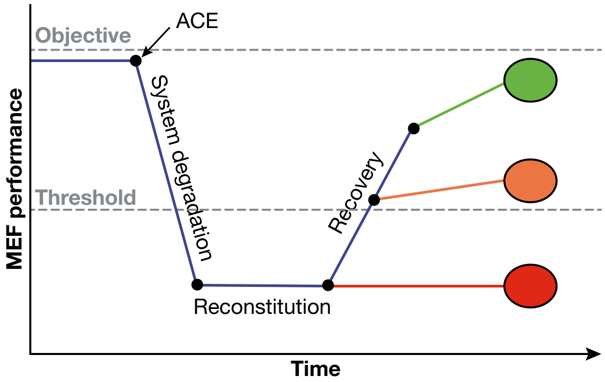


Figure 1. ACE impact on mission essential functions (MEFs) performance. The color-coded outcomes illustrate how the system’s ability to quickly respond to ACEs can determine mission success or failure.

The term *cyber resilience* has many definitions. The Committee on National Security Systems offers this representative definition in its glossary: “The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.”[15] Here the concern spans an assortment of potentially adverse cyber events (ACEs), such as malicious attack, software bugs, component failures, operator errors, and acts of God. Cyber resilience becomes more motivating when we can show how ACEs impact higher-level mission/business functions that depend on cyber. See Figure 1 for a basic illustration of the concept. An ACE can affect missions via impacts on the performance of supporting mission-essential functions (MEFs) provided by a target system. A resilient architecture may allow MEF performance to rise above its associated minimal threshold value.

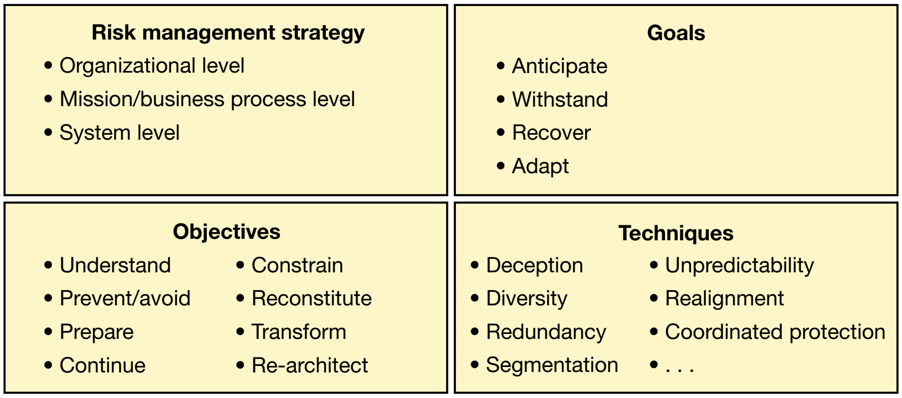
It can be daunting to perform the analysis required to understand multiple MEFs from across a set of supporting cyber systems and how their performance can impact mission threads across a timeline. Monte Carlo simulation is one useful technique.[16]

Cyber Resilience Frameworks

Several cyber resilience frameworks have emerged in recent years. For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework organizes resilience mechanisms into five categories: identify, protect, detect, respond, and recover.[17]

NIST Special Publication 800-160, Vol. 2, “Developing Cyber Resilient Systems: A Systems Security Engineering Approach,”[18] describes a collection of resilience goals, objectives, and techniques/mechanisms, all driven by a risk management strategy (Figure 2).

APL's own Resilient Program Framework emphasizes the need to understand and influence the adversary across a system's life cycle. Furthermore, APL recently dedicated a *Digest* issue to resilience that included articles on cyber resilience principles and best practices.[19]



Risk management strategy

- Organizational level
- Mission/business process level
- System level

Goals

- Anticipate
- Withstand
- Recover
- Adapt

Objectives

- Understand
- Prevent/avoid
- Prepare
- Continue
- Constrain
- Reconstitute
- Transform
- Re-architect

Techniques

- Deception
- Diversity
- Redundancy
- Segmentation
- Unpredictability
- Realignment
- Coordinated protection
- . . .

Figure 2. Cyber resilience constructs. Constituting just one example of recently developed cyber resilience frameworks, these constructs are based on NIST Special Publication 800-160, Vol. 2.[18]

Cyber Resilience Mechanisms

In addition to organizing frameworks, much has been written about specific resilience mechanisms/techniques to implement the resilience concepts suggested by the frameworks. Examples include

- redundancy with diverse implementation,
- hardware-based attestation,
- dynamic changes in connectivity,
- multiple alternative modes of operation,
- automated operating system reimaging, and
- moving target defense (MTD).[20–23]

MTD can be a key component of an active resilience architecture. As Doug Britton states: "This strategy introduces a dynamic, constantly evolving attack surface across multiple system dimensions. . . . prompting attackers to question if the vulnerabilities they find are real or fake, if systems are a decoy and if the layout of a network is genuine."[24]

Another example of coordinated resilience mechanisms appears in Figure 3.[25] The context is a space system that includes a telemetry, tracking, and commanding (TT&C) application for a space vehicle. The application is critical, so system designers arrange for periodic measurement of the application's integrity, including its executable and data files (A in the figure). A monitoring system compares integrity measurements to "known-good" measurements provided by a trusted platform module, or TPM (B). If the integrity measurement indicates a loss of integrity (e.g., as indicated by differing cryptographic hashes computed over the files),

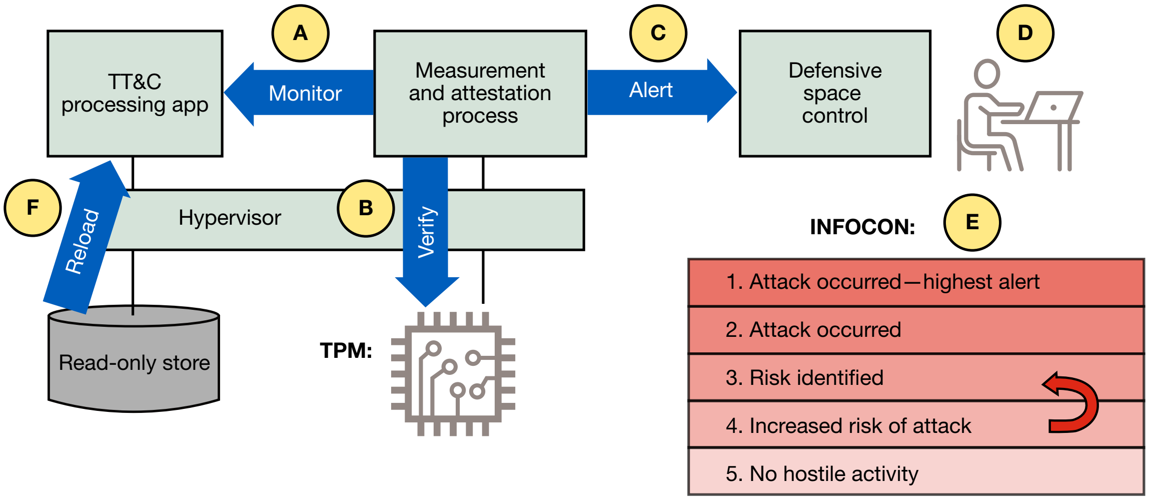


Figure 3. Resilience mechanisms[25] in a system that includes a critical TT&C application for a space vehicle. The application's integrity is monitored (A). Measurements are verified against "known-good" measurements provided by a trusted platform module, or TPM (B). If a loss of integrity is indicated, the measurement module alerts the defensive space control workstation (C). In some cases the operator (D) raises the network's Information Operations Condition (INFOCON) level, which may invoke other resilience mechanisms (E). In any event, the TT&C application and certain data files are reloaded from a read-only memory, returning them to a known-good state (F).

the measurement module alerts the defensive space control workstation (C). Depending on the situation, the operator (D) may raise the Department of Defense INFOCON[26] level of the network (E), which itself may trigger invocation of other resilience mechanisms (e.g., network disconnection). In any event, TT&C files are reloaded from read-only memory to reestablish a known-good state (F).

An extension of the architecture shown in Figure 3 is the partitioning of a system into different modes of operation to enhance resilience. Modes can help ensure mission survival. For example, in 2015, a command loading error caused the New Horizons spacecraft to enter a special "safe mode" used to diagnose and address problems. Operators at APL resolved the issue and brought the spacecraft out of safe mode to resume full operation.[27] This extended space example illustrates that resilience architectures can themselves become complex. Thus, just as with other cybersecurity-related tools, resilience mechanisms add their own complexity and attack surface to a system, and thus must be considered with care.

A final consideration is the use of noncyber mechanisms to cover for cyber-enabled systems in case those systems fail or become distrusted. For example, the US Naval Academy reintroduced celestial navigation training to provide future officers with an alternative means of navigation should cyber-enabled navigation systems, such as GPS, fail.[28]

Cyber Resilience Quantification

While frameworks and implementation mechanisms provide a broad range of resilience options, quantifying the value of any given architecture remains a challenge. Work is proceeding in this area, including ongoing resilience estimation efforts underway at APL.[29–33]

For example, one of the APL approaches[32] is a stochastic discrete-event simulation that computes an overall Resilience Index (RI) for a target system. The simulator executes a large number of trials in which simulated ACEs occur across a mission timeline. The approach defines any trial in which an MEF performance falls below its related threshold as a failed trial. The RI is the ratio of successful trials to total trials attempted.

CYBER RESILIENCE IN THE FUTURE

APL is actively engaged in research on resilience mechanisms and frameworks/architectures that combine them. An example is the Cyber-Resilient Ship research area (Figure 4). Borrowing ideas from zero trust architectures[34–36] and the "Orange Book" concept of the trusted computing base,[37] the Cyber-Resilient Ship research area focuses on exploring ways to

- provide computing architectures that can operate through and recover from cyberattacks;

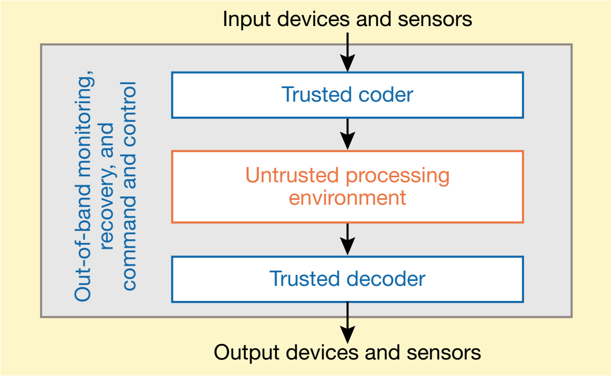

Input devices and sensors
Trusted coder
Untrusted processing environment
Trusted decoder
Output devices and sensors
Out-of-band monitoring, recovery, and command and control

Figure 4. Cyber-Resilient Ship architecture. This research area focuses on investigating ways to provide computing architectures that can operate through and recover from cyberattacks, allow use of possibly compromised components, and include out-of-band functionality to monitor the system and restore mission-critical capabilities.

- allow use of possibly compromised components by using techniques such as (1) homomorphic encryption to execute functions in untrusted processing environments without disclosing the functions or the data that they process, and (2) deploying a small set of trusted components on which missions can depend; and
- include out-of-band functionality to monitor the system and restore mission-critical capabilities.

For the next 2 years, APL will emphasize the development of mission threads that demonstrate the end-to-end SCOCI (Secure Computation on Compromised Infrastructures) approach. The technologies supporting the aspects of the Cyber-Resilient Ship architecture are currently immature and have been developed largely independently. Combining these elements into an end-to-end system will require solving many system compatibility challenges. In addition, applying the techniques to a mission problem will require raising the maturity and abstraction levels of the technologies. Specific research areas aim to achieve the following:

- Reduce the gap between theoretical capabilities and practical, mission-focused application SCOCI primitives such as secure function evaluation (discussed further below) and verifiable computation.
- Develop algorithms and protocols that leverage parallel and distributed computation to provide scalable, asymmetric trade-offs between performance characteristics and increasing the difficulty on the adversary's part in compromising the entire system.
- Migrate endpoint processing and control logic from special-purpose, physical systems to software-defined components executing on commodity infrastructure.

- Develop novel approaches for detection and mitigation of cyber and cyber-physical attacks based on out-of-band monitoring of physical phenomena associated with computation.

To further describe homomorphic encryption, we note that data can exist in three states: at rest, in transit, and in use. Conventional encryption approaches can provide security for data at rest and in transit. However, conventional encryption has not been as helpful for data in-use (in processing). Homomorphic encryption techniques may be able to complement traditional encryption approaches by enabling data in-use processing to be encrypted, thus providing protection for data in all three states (Figure 5).

Specifically, homomorphic encryption enables the concept of secure function evaluation, which allows untrusted processing environments to execute functions but does not allow those environments to learn how those functions work. Homomorphic encryption is computationally intensive, so APL is exploring both full and partial encryption approaches as well as experimenting with different algorithms.

While Cyber-Resilient Ship focuses on naval platforms, the underlying technologies are expected to be widely applied to other critical mission systems. Other related resilience research at APL includes

- achieving reliable data delivery over Internet Protocol (IP) networks in challenging environments (e.g., in the presence of cyberattack, jamming) that does not rely on bidirectional connectivity;

- detecting compromised systems at the instruction level using the Intel Management Engine coprocessor[38] and radio frequency (RF) signatures; and

- using virtualized programmable logic controllers to respond and recover from cyberattack, faulty behavior, and physical damage.

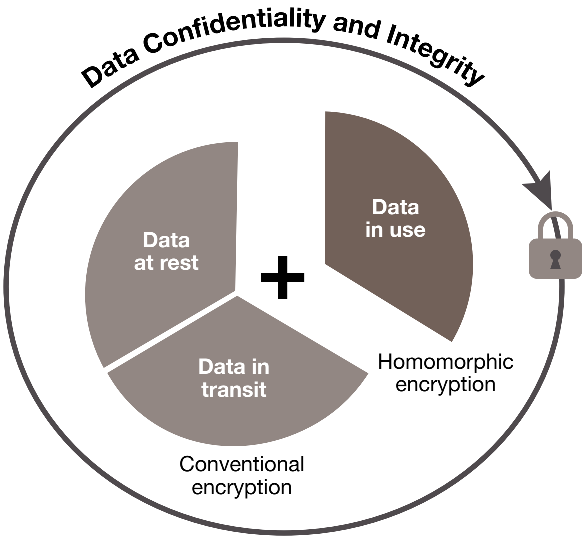


Figure 5. Homomorphic encryption in support of data-in-processing.

CONCLUSION

This article concludes with a speculation on the state of cyber resilience 25 years in the future. This is a naturally hazardous endeavor, but one can begin by noting that the US government and others now consider cyber a distinct domain of battle[39] in which cyber resilience takes on added urgency.

Cyber resilience is expected to grow more sophisticated, supported by a nonlinear increase in machine intelligence over time.[40] Areas such as threat modeling, formal methods, and detection/response capabilities may experience considerable improvements. Quantum computing and machine learning methods may have outsize impacts.[41] For example, one might imagine machine learning capabilities that predict adversary actions at a stage early enough to mount preemptive semi- or fully automated actions.

Ultimately, cyber systems may begin to take on characteristics of biological systems. Similar to ant colonies, armies of nanoscale Internet of Things (IoT) agents may cooperate to achieve resilience goals; of course, the reverse may also be true. Bio-inspired cyber systems may possess digital immune systems,[42] with immune "cells" constantly on patrol, learning and adapting as they encounter pathogens. Autoimmune conditions may result from improperly tuned immune agents. Researchers may develop cyber vaccines for particularly virulent "microbes," an idea that hearkens back to today's antivirus software but in a more "evolved" setting.

The asymmetric advantage that attackers enjoy today may begin to erode as cyber systems evolve novel defenses under selective pressure. Here we may see the emergence of a new professional job category for humans: cyber husbandry, a field where automation-assisted specialists manage the selective breeding of ever-more resilient cyber organisms. More outlandishly, the tables may take a dystopian turn, with now-dominant, highly intelligent cyber systems adopting a resilience strategy —Matrix[43] style— that incorporates humans bred for lethality and obedience. One can only hope that such a scenario remains squarely in the realm of science fiction.

REFERENCES

[1] Verizon, "2019 data breach investigations report," 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

[2] Defense Science Board, "Task force report: Resilient military systems and the advanced cyber threat," Department of Defense, Washington, DC, 2013, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf.

[3] C.-S. Chan, “Complexity the worst enemy of security,” *Schneier on Security*, Dec. 17, 2012, https://www.schneier.com/news/archives/2012/12/complexity_the_worst.html.

[4] S. Chong, J. Guttman, A. Datta, A. Myers, B. Pierce, et al., “Report on the NSF Workshop on Formal Methods for Security,” Technical Report, National Science Foundation, Alexandria, VA, Aug. 1, 2016, https://people.csail.mit.edu/nickolai/papers/chong-nsf-sfm.pdf.

[5] W. Arthur and D. Challener, *A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security*, New York: Apress, 2015, https://link.springer.com/book/10.1007%2F978-1-4302-6584-9.

[6] O’Hearn, P. W., “Continuous reasoning: Scaling the impact of formal methods,” in *Proc. 33rd Annu. ACM/IEEE Symp. on Logic in Comput. Sci.*, 2018, https://doi.org/10.1145/3209108.3209109.

[7] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, “The emperor’s new security indicators,” in *Proc. 2007 IEEE Symp. Security and Privacy*, 2007, pp. 51–65, https://doi.org/10.1109/SP.2007.35.

[8] D. M. Sarno, J. E. Lewis, C. J. Bohil, and M. B. Neider, “Which phish is on the hook? Phishing vulnerability for older versus younger adults,” *Hum. Factors*, vol. 62, no. 5, pp. 704–717, 2019, https://doi.org/10.1177/0018720819855570.

[9] “Google Application Security.” Google. 2019. https://www.google.com/about/appsecurity/android-rewards/ (accessed Sep. 15, 2020).

[10] US Department of Defense, “Department of Defense expands ‘Hack the Pentagon’ crowdsourced digital defense program,” press release, Oct. 24, 2018, https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/.

[11] O. H. Alhazmi, Y. K. Malaiya, and I. Ray, “Measuring, analyzing and predicting security vulnerabilities in software systems,” *Comput. Secur.*, vol. 26, no. 3, pp. 219–228, 2007, https://doi.org/10.1016/j.cose.2006.10.002.

[12] T. Llanso and M. McNeil, “Estimating software vulnerability counts in the context of cyber risk assessments,” in *Proc. 51st Hawaii Int. Conf. Syst. Sci. (HICSS-51)*, 2018, pp. 1–7, https://scholarspace.manoa.hawaii.edu/bitstream/10125/50576/1/paper0689.pdf.

[13] PCI Security Standards Council, “Payment Card Industry (PCI) Data Security Standard 139,” PCI Security Standards Council, Wakefield, MA, May 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.

[14] “Cybersecurity Maturity Model Certification.” US Department of Defense, 2019. https://www.acq.osd.mil/cmmc/index.html.

[15] Committee on National Security Systems, “National information assurance (IA) glossary,” CNSS Instruction No. 4009, CNSS, Washington, DC, Apr. 26, 2010, https://www.hsdl.org/?abstract&did=7447.

[16] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, “Computing the impact of cyber attacks on complex missions,” in *Proc. 2011 IEEE Int. Syst. Conf.*, Montreal, QC, 2011, pp. 46–51, https://doi.org/10.1109/SYSCON.2011.5929055.

[17] NIST. “Cybersecurity Framework,” Version 1.1. Apr. 16, 2018. https://www.nist.gov/cyberframework.

[18] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, “Developing cyber resilient systems: A systems security engineering approach,” NIST Special Publication 800-160, Vol. 2, NIST, Gaithersburg, MD, Nov. 2019, https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final.

[19] “A Snapshot of Engineering for Resilience at APL,” *Johns Hopkins APL Tech. Dig.*, vol. 34, no. 4, pp. 419–540, 2019, https://www.jhuapl.edu/TechDigest/Detail?Journal=J&VolumeID=34&IssueID=4.

[20] H. Okhravi, J. W. Haines, and K. Ingols, “Achieving cyber survivability in a contested environment using a cyber moving target,” *High Frontier*, vol. 7, pp. 9–13, 2011, http://web.mit.edu/ha22286/www/papers/HF11.pdf.

[21] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Başar, “Resilient control of cyber-physical systems against denial-of-service attacks,” in *Proc. 2013 6th Int. Symp. Resilient Control Syst. (ISRCS)*, San Francisco, CA, 2013, pp. 54–59, https://doi.org/10.1109/ISRCS.2013.6623750.

[22] Y. Hayel and Q. Zhu, “Resilient and secure network design for cyber attack-induced cascading link failures in critical infrastructures,” in *Proc. 2015 49th Annu. Conf. Inf. Sci. Syst. (CISS)*, Baltimore, MD, 2015, pp. 1–3, https://doi.org/10.1109/CISS.2015.7086855.

[23] T. Llanso and D. Pearson, “Achieving space mission resilience to cyber attack: Architectural implications,” in *Proc. AIAA Space 2016*, Long Beach, CA, 2016, pp. 1–12, https://doi.org/10.2514/6.2016-5604.

[24] D. Britton, “3 reasons why moving target defense must be a priority,” *GCN*, Jun. 10, 2019, https://gcn.com/articles/2019/06/10/moving-target-defense.aspx.

[25] F. Belz and T. Llanso, “Aerospace Report No. TOR-2012(8960)-7: Space Mission Resilience to Cyber Attacks,” 2012.

[26] US Strategic Command, “Department of Defense (DoD) Information Operations Condition (INFOCON) system procedures,” Strategic Command Directive (SD) 527-1, Jan. 27, 2006, https://info.publicintelligence.net/StrategicCommandDirective527-1_27JAN2006InformationOperationsCondition-INFOCON-System.pdf.

[27] NASA, “New Horizons exits brief safe mode, recovery operations continue,” Feb. 10, 2017 (updated Aug. 6, 2017), https://www.nasa.gov/feature/new-horizons-exits-brief-safe-mode-recovery-operations-continue.

[28] T. Prudente, “Naval Academy reinstates celestial navigation,” *Military Times*, Nov. 1, 2015, https://www.militarytimes.com/news/your-military/2015/11/01/naval-academy-reinstates-celestial-navigation.

[29] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and Alex Kott, “Resilience metrics for cyber systems,” *Environ. Syst. Decis.*, vol. 33, pp. 471–476, 2013, https://doi.org/10.1007/s10669-013-9485-y.

[30] D. Bodeau and R. Graubert, “Cyber resilience metrics: Key observations,” MITRE Corp., Bedford, MA, 2016, https://www.mitre.org/sites/default/files/publications/pr-16-0779-cyber-resilience-metrics-key-observations.pdf.

[31] A. Dwivedi, “Implementing cyber resilient designs through graph analytics assisted model based systems engineering,” in *Proc. IEEE Int. Conf. Softw. Qual., Rel. and Secur. Companion*, Lisbon, 2018, pp. 607–616, https://doi.org/10.1109/QRS-C.2018.00106.

[32] T. Llanso and M. McNeil, “Towards an organizationally-relevant quantification of cyber resilience,” in *Proc. 54th Hawaii Int. Conf. Syst. Sci. (HICSS-54)*, Jan. 5–8, 2021 (forthcoming).

[33] C. A. Smith and T. J. Allensworth, “Quantifying system resilience using probabilistic risk assessment techniques,” *Johns Hopkins APL Tech. Dig.*, vol. 34, no. 9, pp. 471–479, 2019, https://www.jhuapl.edu/Content/techdigest/pdf/V34-N04/34-04-Smith-PRA.pdf.

[34] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, NIST, Gaithersburg, MD, 2019, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[35] US Department of Defense, “DoD Digital Modernization Strategy: DoD information resource management strategic plan FY19–23,” Washington, DC: Department of Defense, Jul. 12, 2019, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/dod-digital-modernization-strategy-2019.pdf.

[36] Kiwi (community team member), “What is zero trust?” Palo Alto Networks blog, Oct. 10, 2019, https://live.paloaltonetworks.com/t5/blogs/what-is-zero-trust/ba-p/292327.

[37] US Department of Defense, “Department of Defense trusted computer system evaluation criteria,” DoD 5200.28-STD, Department of Defense, Washington, DC, Aug. 15, 1983, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf.

[38] Intel.“Support, Intel® Management Engine.” https://www.intel.com/content/www/us/en/support/products/34227/software/chipset-software/intel-management-engine.html (accessed Nov. 12, 2020).

[39] J. T. Bennett, “Pentagon declares the Internet a war domain,” *The Hill*, Jul. 14, 2011, https://thehill.com/policy/technology/171531-pentagon-declares-the-internet-a-domain-of-war.

[40] W. Holt, “Moore’s law: A path going forward,” in *Proc. 2016 IEEE Int. Solid-State Circuits Conf. (ISSC)*, San Francisco, CA, 2016, pp. 8–13, https://doi.org/10.1109/ISSCC.2016.7417888.

[41] L. Columbus, “Why AI is the future of cybersecurity,” *Forbes*, Jul. 14, 2019, https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity.

[42] D. Dasgupta, “Immuno-inspired autonomic system for cyber defense,” *Inf. Secur. Tech. Rep.*, vol. 12, no. 4, pp. 235–241, 2007, https://doi.org/10.1016/j.istr.2007.10.002.

[43] A. Wachowski and L. Wachowski (dir.), *The Matrix*, Warner Brothers, 1999.

Thomas H. Llansó, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Thomas H. Llansó is on the Principal Professional Staff at APL where he conducts applied research in cyber-related analytics (e.g., for risk analysis, resilience analysis, mitigation selection). He has a BS in computer science from the College of William & Mary, a master's in computer science from Johns Hopkins University, and a doctorate in information systems from Dakota State University. He taught for 12 years in the Johns Hopkins University Whiting School of Engineering and served as a student adviser for 9 years. In addition, he is a track co-chair for cybersecurity at the Hawaii International Conference on System Sciences. His email address is thomas.llanso@jhuapl.edu.

Daniel A. Hedgecock, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Daniel A. Hedgecock is a cybersecurity situational awareness developer and analyst, an assistant group supervisor, and a project manager in APL's Asymmetric Operations Sector. He has a BS in applied physics from Grove City College and an MS in applied physics from Johns Hopkins University. He has an extensive background leading and executing studies and analyses, in both the Air and Missile Defense and the Cyber Operations Mission Areas at APL. His email address is daniel.hedgecock@jhuapl.edu.

J. Aaron Pendergrass, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

J. Aaron Pendergrass is the chief scientist for APL's Enterprise Systems Cyber Research Group, the research area lead for assured critical missions within APL's Cyber Operations Mission Area, and director of APL's Software Assurance Research and Applications (SARA) laboratory. He has a BA in computer science from Oberlin College and an MS in computer science from University of Maryland, College Park. He has 13 years of experience researching static source code and binary analysis, formal verification, and operating system integrity. His email address is james.pendergrass@jhuapl.edu.