Atlantic Council

Operationalizing a Cybersecurity Strategy for the United States

Part II—Scaling resilience through safe coding and trusted architectures

Franklin D. Kramer, Robert J. Butler, and Melanie J. Teplinsky

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

January 2026

Contents

I. Introduction and summary

As described in Part I of this two-part report, a fundamental approach of the Trump administration is ensuring and enhancing the defense of the US homeland. Border security has accordingly been prioritized, and a "Golden Dome" missile defense has been proposed. But equivalent to the challenges of the border and of missile defense is the defense of the information and operational technology systems upon which the national security, economy, and public safety of the United States depend. This report focuses on technology and architectures, and its companion report (Part I) focuses on operations and governance. Together, they identify the challenges facing the United States and describe a proposed national cybersecurity strategy that encompasses key roles for the government and the private sector.

The proposed strategy is built on two components: establishing an operational road map for defensive and offensive campaigning with appropriate roles for government and the private sector; and accelerating the development and adoption of safe coding and zero trust architectures (ZTAs) for key critical infrastructure systems and enterprises. By accomplishing these two sets of activities, the United States will establish a homeland defense cyber posture that provides the president and the national leadership with the necessary capabilities to deter and counter nation-state and criminal adversaries in cyberspace.

Specifically, as set forth in this report, achieving and maintaining that homeland defense cyber posture will require several steps:

- **Enhance the security of software code base for key critical infrastructures** (because unsecured or unsafe code bases present the greatest attack surface for hackers).[1]
  - Utilize formal methods to develop and maintain high-assurance software for information and operational technology (IT and OT) systems of key critical infrastructures that are identified as "Section 9" companies, which are companies "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."2
  - Organize a task force consisting of government and private-sector experts to support use of formal methods to improve software security in each sector that includes Section 9 companies.
  - Engage highly capable private-sector companies as members of the task force, selecting those currently using formal methods: effective, beneficial techniques to vastly reduce software vulnerabilities (as discussed in section III). Their participation will be highly important in supporting prompt and effective utilization of formal methods for Section 9 companies. To the extent that resource or other constraints limit an immediate transition to code written via formal methods, utilize memory safe languages as an initial step along the formal methods spectrum.
  - Support the development and adoption of key cybersecurity technology projects focused on safe coding through formal methods and memory safety that are being undertaken by the Defense Advanced Research Projects Agency (DARPA).
  - Support the development and adoption of artificial intelligence technologies (including generative, agentic, and neuro-symbolic AI powered by large language models, or LLMs) to support the implementation of effective security solutions, including checking proofs for those solutions through formal methods.
- **Establish trusted architectures** (necessary as ill-structured architectures provide multiple vulnerabilities for adversaries to exploit).[3]
  - Establish and/or review regulatory requirements for ZTAs for Section 9 companies in key sectors, with the national cyber director providing overall coordination/harmonization and the sector risk management agencies generating specific regulatory requirements.
  - Organize a task force consisting of government and private-sector experts to generate the technical requirements for, and to support, the establishment of zero trust architectures for each sector that includes Section 9 companies. The actual ZTA implementation activities would be provided through a combined effort of the Section 9 company and outside private-sector expert assistance.
  - Develop and/or utilize advanced capabilities including ephemeral authentication, postquantum cryptography, enhanced software segmentation, and agentic AI to support zero trust architectures.
  - Organize the establishment of ZTAs across the "regional resilience districts" in key geographic areas (described in the Part I report). Begin by establishing ZTA pilot programs for key port cities, ideally where there are significant military installations, such as in Charleston; these programs should focus on zero trust architectures for key capabilities including local governance.

- **Provide financial assistance.** Recipients should include each Section 9 company and regional resilience district undertaking the establishment of ZTAs. The assistance should include direct funding and/or tax credits to support the initial effort, upgrades, maintenance, and possibly matching federal funds for state-funded initiatives.

While this report identifies several existing technological and architectural improvements that could bolster critical infrastructure cybersecurity, the rapid pace of change necessitates—and we have attempted to set forth—a set of organizational structures and repeatable processes that could be used to accelerate the development and adoption of future cyber "solutions." These include not only the structures and processes necessary to leverage cutting-edge private- and public-sector expertise for the benefit of critical infrastructure cybersecurity, but also the incentives (e.g., funding and liability protections) necessary to spur private-sector cooperation and the sustained multiyear funding necessary to retain and grow the research and development base essential to securing critical infrastructure.

II. The cybersecurity challenge: Unsafe code and insecure architectures

The cybersecurity challenges from adversaries including the People's Republic of China (PRC), the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea (i.e., North Korea), and cyber criminals are set forth in the Part I companion report on operations and are included in the Part II Appendix. The discussion below focuses more specifically on challenges from unsafe code and insecure architectures. As important as the operational road map proposed in Part I will be, without resilient systems and enterprises the United States will not be able to counter adversaries let alone deter their actions. Effective defense has always been a critical element of successful security strategy. As Sun Tzu classically said, "The skillful warriors first made themselves invincible," a comprehensible task since "invincibility depends on oneself." Now, however, far from invincible, American critical national security and commercial systems are at extraordinary risk with adversaries exploiting the multitude of vulnerabilities in software in those systems as well as the often-poor authentication and confidentiality capabilities of networked enterprises that allow key critical systems to interoperate.

The vulnerabilities arise from two main sources: unsafe code and untrustworthy networks.

Unsafe code

So-called memory-safety errors[4] have been described as "today's biggest attack surface for hackers." As the Cybersecurity and Infrastructure Security Agency (CISA) has stated, over two-thirds of software vulnerabilities have historically arisen from the use of memory unsafe code.[5] For over half a century, software engineers have known malicious actors could exploit a class of software defect called "memory safety vulnerabilities" to compromise applications and systems. During that time, experts have repeatedly warned of the problems associated with memory safety vulnerabilities. In a blog post, Microsoft reported that "~70% of the vulnerabilities Microsoft assigns a CVE [Common Vulnerability and Exposure] each year continue to be memory safety issues." Google likewise reported that "the Chromium project finds that around 70% of our serious security bugs are memory safety problems." Mozilla reports that in an analysis of security vulnerabilities, "of the 34 critical/high bugs, 32 were memory-related."[6]

While some recent analysis indicates that the overall percentage of errors from unsafe languages is "only" about 50 percent,[7] the situation is worsening for critical infrastructures. As one report underscored, critical infrastructures are at high risk from memory-safety issues: "Recently, nation-state actors, such as Volt Typhoon, have demonstrated the potential real-world impact of memory safety vulnerabilities in the software used to run critical infrastructure."[8] According to that review, "in the last few years, memory safety vulnerabilities within ICS [industrial control systems] have seen a steady upward trend. There were less than 1,000 CVEs in 2014 but nearly 3,000 in 2023 alone."[9]

The problem has arisen because so much programming utilizes programming languages like C and C++. While very efficient, such languages are susceptible to adversarial attacks that exploit their inherent unprotected excess "memory space," which allows an adversary to insert malware into a program.[10] As one earlier Atlantic Council study described:

> These languages are well suited to systems programming, giving instructions directly to the guts of a machine to produce programs with very fast performance. That freedom also creates risk, allowing a variety of bugs like buffer overflows, memory leaks, dangling pointers, etc. These issues, called memory-safety errors, can result from simple typos and forgotten lines of code or from complex memory structures and unforeseen interactions.[11]

The lack of built-in memory-safety mechanisms affords adversaries the opportunities to violate data confidentiality, integrity and availability. In short, as a recent report from CISA and the National Security Agency states, "The importance of memory safety cannot be overstated."[12]

Zero trust challenges

Effective techniques for cybersecurity of critical infrastructures require the implementation of zero trust architectures. A ZTA has five components:

- Authentication of the user.
- Authorization for the user to do what is being undertaken.
- Segmentation of the network so that compromise of one area does not allow compromise of others.
- Encryption of data.
- Continuous monitoring of the network for compromises.[13]

The failure to implement zero trust requirements has been instrumental in enabling or supporting adversary breaches. For example, in the well-known Colonial Pipeline attack, the absence of proper authentication—specifically, the lack of multifactor authentication on a VPN account—was a key factor in enabling the breach.[14] As other examples, absence of segmentation controls led to significant breaches at "22 energy operators responsible for various aspects of the Danish energy infrastructure,"[15] and the British Library suffered significant data losses since its system "didn't have a way to immediately stop lateral movements."[16]

Analytically, adopting these components into ZTAs for critical infrastructures is a well understood process. By way of examples, the Cloud Security Alliance has promulgated the *Zero Trust Guidance for Critical Infrastructure*;[17] the North American Electric Reliability Corporation has issued a white paper entitled "Zero Trust Security for Electric Operations Technology;"[18] and private cybersecurity providers including Xage Security, Dragos, and Fortinet also have expertise in the process required to migrate electric utility and other critical information and operational technology (IT/OT) systems to ZTA platforms.[19]

Likewise, to support the practicalities of ZTA implementation for critical infrastructures, the National Institute of Standards and Technologies (NIST), working with private-sector cybersecurity companies through the National Cybersecurity Center of Excellence, has demonstrated numerous ZTA solutions. NIST describes these as "practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges," noting that they are established by developing "modular, adaptable example cybersecurity solutions using commercially available technology."[20]

The NIST efforts set forth architecture descriptions and provide specific examples utilizing multiple available commercial components. NIST further undertook red-team testing to demonstrate that the described architectures would be resilient against adversary cyberattack.[21] The results demonstrated that a properly configured zero trust architecture could establish significant resilience for both IT and OT networks. As one example, the testing for electric utilities and the oil and gas industry successfully accomplished a spectrum of cybersecurity tasks important to zero trust including: detecting new devices on the network; recognizing new vulnerabilities and engaging in patch management; recognizing loss of devices from the network; detecting anomalous communications; and monitoring devices with cellular connectivity to the network.[22]

However, while ZTAs are easily described in the abstract and the required capabilities do exist and can be demonstrated in a laboratory setting (as NIST has shown), they are far more difficult to put into practice at scale in the government or large bureaucracies. By way of example, even the Department of Defense, which has both significant funding and substantial expertise, has yet to fully implement ZTA. The current target implementation date for IT systems is 2027.[23] While DOD has validated several ZTA solutions for IT—including Thunderdome,[24] Flank Speed,[25] and Fort Zero[26]--which are being adopted by multiple DoD organizations, departmental-wide adoption is yet to be accomplished. Moreover, while DoD recently released guidance for implementing ZT for OT,[27] the ZT implementation timeframe for OT systems has yet to be established, though recent statements indicate an initial target of 2030 for some systems, with others following by several years.[28]

The reasons for the disparity between the well-understood analytic capability and the on-the-ground reality derives from a series of factors. Perhaps most relevantly, Section 9 companies in key sectors will, in addition to their corporate activities, generally be running operational technology systems required for the provision of their services. As the Cloud Security Alliance has described, the scale, complexity, longevity, and legacy nature of many operational technology systems make it more difficult to implement ZTA solutions.[29] Another report similarly elaborated that "many OT organizations struggle to implement zero trust seamlessly" due to inclusion of legacy technology, a lack of standardization, and the time it takes to respond to an attack potentially leading to "production loss or interruption of critical infrastructure that may lead to serious health and safety risks."[30] A third report likewise noted the difficulty of making "ZTA technologies compatible with the legacy technologies found in the OT environments," adding that the "OT component (e.g., programmable logic controllers) may not support the technologies or protocols required to fully integrate with a ZTA system."[31]

III. Cybersecurity technology road map: Scaling resilience through safe coding and ZTAs

Safe coding

Safe coding can be accomplished through formal methods (described below) and, to an important but lesser degree, use of memory safe languages. The discussion that follows describes each of these approaches as well as existing DARPA initiatives to make such capabilities widely available.

Formal methods: Approach and benefits

Formal methods "mathematically prove that code is error-free and works as specified."[32] DARPA has described formal methods as "mathematically rigorous techniques that create mathematical proofs for developing software that eliminate virtually all exploitable vulnerabilities."[33] Accordingly, "successfully applying formal methods provides many benefits," including early identification and provable eradication of software bugs and full integration of ZTA approaches.[34]

Formal methods have long been recommended or required in safety-critical systems such as those found in the automotive,[35] aerospace,[36] medical,[37] and nuclear power[38] industries. Despite their value, formal methods have not been more widely adopted in industry because of a "reputation for requiring a huge amount of training and effort to verify a tiny piece of relatively straightforward code, so the return on investment is justified only in safety-critical domains,"[39] such as medical systems and avionics.

However, Amazon Web Services (AWS) engineers, utilizing two programming languages—TLA+ and PlusCal—found "this perception to be wrong."[40] Using this approach for "large complex real-world systems" demonstrated:

> TLA+ has added significant value, either finding subtle bugs we are sure we would not have found by other means or giving us enough understanding and confidence to make aggressive performance optimizations without sacrificing correctness. Amazon now has . . . teams using TLA+, with encouragement from senior management and technical leadership. Engineers from entry level to principal have been able to learn TLA+ from scratch and get useful results in two to three weeks, in some cases in their personal time on weekends and evenings, without further help or training.[41]

This AWS account is from a 2015 article;[42] since then, the company has significantly expanded its use of formal methods.[43] However, as AWS engineers more recently observed:

> Despite significant success in scaling formal and semi-formal testing methods across AWS over the past 15 years, several challenges persist, particularly in industrial adoption of formal methods. The primary barriers for formal methods tools include their steep learning curve and the specialized domain expertise required. Additionally, many of these tools remain academic in nature and lack user-friendly interfaces.[44]

From AWS's extensive use of formal methods and the cautionary language above, one can see that formal methods are entirely available and highly useful so long as the relevant level of expertise can be engaged. This conclusion is buttressed by the impressive list of highly capable companies using formal methods (both inside and outside safety-critical domains),[45] including Airbus,[46] ASML,[47] BAE,[48] Arm Holdings,[49] Boeing,[50] FireEye,[51] Intel,[52] and Microsoft.[53] For example, Airbus has used Astrée, a high-end formal methods tool, in the development of safety-critical software for various planes including the A380, beginning in 2003 when Astrée was used to prove the absence of any runtime errors in the fly-by-wire primary flight-control software of an Airbus A340. Formal methods analysis, supported by expert capabilities, also has been conducted successfully on several widely used internet protocols including: the transport layer security (TLS) protocol (versions 1.2 and 1.3),[54] which is the principal means for securing internet communication; a critical protocol for secure communication on 5G networks known as 5G authentication and key agreement (5G-AKA);[55] and the worldwide standard for smartcard payments, known as EMV after its founders, Europay, Mastercard, and Visa.[56] Formal methods also have been used to demonstrate software "correctness,"[57] which is key to the development of safety- and mission-critical systems.[58]

As the foregoing demonstrates, formal methods are in consequential use by key companies and in high-assurance contexts. However, perhaps the most relevant demonstration of the value of formal methods to operational technology systems comes from the DARPA High-Assurance Cyber Military Systems (HACMS) demonstrations.

> DARPA tested the software developed under HACMS on real military hardware and systems to verify its performance and compatibility in operational environments. First using a small quadcopter as a testbed, then graduating to a much larger helicopter, Boeing's Unmanned Little Bird, DARPA demonstrated the benefits of software written with formal methods. HACMS conducted simulated cyber-attacks (often called red team exercises) to test the resilience of its software against real-world threats. These exercises identified weaknesses

> and vulnerabilities that could be addressed before deployment. . . .
>
> When the project started, the Red Team was able to remotely take over the systems. At the end of the HACMS program, they repeated that experiment while Little Bird was in flight with two test pilots on board. DARPA's HACMS team had become so confident in the formally verified software that they were willing to risk the lives of those two pilots as the Red Team attempted to hack the helicopter—the Red Team failed, and the pilots remarked they couldn't even tell the difference in flying the high assurance version. To this day, the system has yet to be successfully hacked.[59]

Given, on the one hand, the multiple attacks on critical infrastructures and, on the other, the success Amazon and other companies and especially the HACMS demonstration have had in using formal methods, a high priority should be placed on an effort to ensure that essential code for Section 9 companies is written by formal methods.

Assuming a determination to go forward, a Section 9 company would, of course, be able to choose from the full spectrum of the private-sector support in undertaking the implementation of formal methods. Given the importance of ensuring the highest degree of cybersecurity for Section 9 companies, however, an additional valuable resource should be created by the government by establishing a public-private team—a Formal Methods Task Force—to work with and serve as a resource for Section 9 companies in generating IT and OT code written pursuant to formal methods. Not all Section 9 companies will need the Formal Methods Task Force support, but that task force could be available to provide support if and as useful. Such support likely will be essential to at least some efforts to ensure that code for OT for Section 9 companies is written using formal methods.

Formal Methods Task Force: Setting its membership and charge

A Formal Methods Task Force would leverage the National Cyber Labs Cohort, comprised of experts from federally funded research and development centers (FFRDCs), university affiliated research centers (UARCs), the National Laboratories, and industry experts operating as special government employees under the oversight of the Cybersecurity and Infrastructure Security Agency's director and working with the relevant sector risk management agency. The task force would have a core membership complemented for each sector with sector experts. It would be charged initially with writing or helping to write IT and OT code via formal methods for designated Section 9 companies.

Finally, as discussed in more detail below, an additional recommendation of this report is to establish a task force that can support zero trust architectures for Section 9 companies. **Inasmuch as that task force and the proposed formal methods task force will have overlapping focus on Section 9 companies, it will be sensible for there to be a single task force with the formal methods and zero trust elements included within so there can be appropriate coordination with the Section 9 companies as well as coordination of expertise.**

In addition to the proposed Formal Methods Task Force, there are several ongoing developmental efforts that may increase the use of formal methods.

Using formal methods to upgrade existing systems

On the DARPA front, these efforts include using formal methods in upgrading existing systems. These computer programs can regularly benefit from improvements in performance or security by upgrades that "enhance and replace components of existing software with more secure and more performant code."[60] There are risks in undertaking such actions, however, since "introducing enhancements or replacements into large legacy code bases carries a high risk that new code will not safely compose with the rest of the system,"[61] and thereby provide opportunities for adversarial attacks.

DARPA has established the V-SPELLS program to overcome those issues by utilizing formal methods. The V-SPELLS program "will create practical tools for developers to gain benefits of formal software verification in incremental software (re) engineering."[62] The goal is to:

> Create a developer-accessible capability for piece-by-piece enhancement of software components with new verified code that is both correct-by-construction and compatible- by-construction, i.e., safely composable with the rest of the system.[63]

In short, V-SPELLS will allow for upgrading code without generating new vulnerabilities. The V-SPELLS capability is now undergoing practical testing and evaluation with the military services.[64] If it works as expected, the capability will be available for widespread usage both for national security and commercial activities.

Making formal methods tools and solutions available to all developers

In addition, DARPA is trying to make formal methods technologies, tools, and solutions available to all developers for accomplishing safe coding. As noted above, there is a widespread belief that formal methods require highly qualified specialized programmers and large-scale commitments of time—one reason why the capability is not in widespread use. To overcome these difficulties, DARPA has now established the PROVERS program to "develop formal methods tools to guide software engineers through designing proof-friendly software systems and reduce the proof repair workload."[65] The program's goal "is to make formal methods accessible to non-experts (e.g., traditional software developers and systems engineers) while minimizing the impact on their existing processes and performance."[66] PROVERS is a forty-two-month program and, as of this writing, about halfway through its timeframe. Its effective completion will help significantly change the programming landscape by adding to the capability for safe coding. The program and the activities by private-sector companies like AWS in using formal methods should help encourage widespread usage.

Finally, AI advances should support the utilization of formal methods for operational technologies. As AWS engineers have observed:

> Looking ahead, we believe large language models and AI assistants will significantly help address the adoption challenges of formal methods in practice. Just as AI-assisted unit testing has gained popularity, these tools are expected soon to help developers create formal models and specifications, making these advanced techniques more accessible to the broader developer community.[67]

While such an approach is not yet available, the Formal Methods Task Force could help develop it. Illustratively, Microsoft is looking at using LLMs to make it easier to develop proof with a tool called Verus to "formally verify Rust programs,"[68] referring to a memory-safe language.

Memory safe languages

Memory safety is a critical and time-consuming issue. As CISA has stated:

> Despite software manufacturers investing vast resources attempting to mitigate memory safety vulnerabilities, they remain pervasive. Customers must then expend significant resources responding to these vulnerabilities through both onerous patch management programs and incident response activities.[69]

Absent moving to code written by formal methods, CISA said, the "most promising mitigation is for software manufacturers to use a memory safe programming language because it is a coding language not susceptible to memory safety vulnerabilities."[70]

Some companies already have begun the transition to memory safe languages (MSLs), as discussed in the Atlantic Council's 2022 *Buying Down Risk* series.[71] For example, Google has adopted an "incremental approach focusing on replacing new and highest risk existing code," aiming to both maximize benefits and minimize the level of effort.[72] This approach has resulted in a dramatic drop in the percentage of memory-safety vulnerabilities in Android from 76 percent to 24 percent over six years.[73]

At the same time, in *The Case for Memory Safe Roadmaps*, CISA and its domestic and foreign partners underscored the cost of embracing memory-safe languages:

> The authoring agencies acknowledge the commercial reality that transitioning to MSLs will involve significant investments and executive attention. Further, any such transition will take careful planning over a period of years. Although there is an upfront cost in migrating codebases to MSLs, these investments will improve product reliability, quality, and—critically—customer security.[74]

It bears emphasizing that adopting high-assurance software development techniques, whether formal methods or memory-safe coding, not only improves security but, by eliminating entire classes of software bugs earlier in the development pipeline, can also decrease costs (e.g., by avoiding delays due to discovery of a vulnerability down the road while testing software deployment on physical hardware).

The federal government has developed a road map for companies to utilize in moving to memory-safe languages,[75] but it does not have a sense of urgency and, given the multiple attacks on key critical infrastructures, prompt transition for Section 9 companies is important.

One key activity that could speed the transition is DARPA's TRACTOR program,[76] which "aims to automate the translation of legacy C to Rust."[77] The explicit goal of the TRACTOR program is to "achieve the same quality and style that a skilled Rust developer would produce, thereby eliminating the entire class of memory safety security vulnerabilities present in C programs."[78]

TRACTOR is in its early days of use, but the widespread use of TRACTOR to transition to RUST would be a significant step to more effective cybersecurity.[79]

Reducing vulnerabilities in critical codebases at speed and scale

Making the above-described foundational changes will pay significant cybersecurity dividends, but it will take time. In the interim, advanced technologies should be tapped to accelerate efforts to find and patch vulnerabilities in the software that undergirds our most critical systems. For example, the AI-powered cyber-reasoning systems[80] developed in connection with DARPA's recent AI Cyber Challenge[81] are capable of finding and patching vulnerabilities in the open-source software[82] that underpins much of our critical infrastructure—doing so at speed and scale. These AI-powered systems "create valuable bug reports and patches for a fraction of the cost of traditional methods,"[83] successfully identifying 77 percent of the competition's synthetic vulnerabilities and patching 61 percent of those identified.[84] While these systems no doubt will be further refined, DARPA already is working to disseminate the technology, which has been open sourced and is available for integration into the critical infrastructure software-development process.

Other efforts include Google's Project Big Sleep, an AI agent that "actively searches and finds unknown security vulnerabilities in software."[85] According to Google, Big Sleep recently found "a critical security flaw . . . known only to threat actors," reportedly marking "the first time an AI agent has been used to directly foil efforts to exploit a vulnerability in the wild." [86] An Integrated Cybersecurity Providers Corps (ICPC) could work to make tools of this sort available to Section 9 companies to accelerate their progress toward a secure software base.

Accelerated development and deployment of advanced technologies (with appropriate safeguards), together with adoption of formal methods and memory-safe languages, would be important steps toward achieving resilience at scale for key critical infrastructure software.

ZTAs: Creating an operational and near-term road map for rapid implementation and sustainment

Establishing zero trust architectures for Section 9 companies will require a significant effort. Three key elements will be needed: deconflicted and harmonized requirements across sectors; establishing a zero trust task force; and utilizing advanced technologies.

Coordinated and harmonized requirements

While the cyber threat from adversary nations and criminals is longstanding, the reality is that most companies, including those associated with key critical infrastructures, have not adopted sufficiently capable cybersecurity technologies and techniques to provide resilient protection. The widespread intrusions exemplified by Volt Typhoon and other Chinese cyberattacks (e.g., in January 2025, the FBI deleted a different Chinese malware from more than 4,000 US computers[87]) underscore that companies on their own often do not sufficiently prioritize cybersecurity. Regulation is needed, just as it was a generation ago to make automobiles safer and to ensure clean air and clean water. At the same time, to avoid undue burden on the private sector, cybersecurity regulations should be effectuated in a reasonable fashion both technically and financially—and appropriately harmonized within and across sectors and with existing regulations,[88] through consultation with the national cyber director and the director of the Office of Management and Budget, who are leading current cybersecurity regulatory harmonization efforts.[89]

To accomplish the level of cybersecurity most relevant to US national and economic security, a sensible starting place for streamlined regulation is with the Section 9 companies engaged in key critical infrastructures. The relevant sectors would include, at a minimum, the electric grid; pipelines; transportation (air, rail, ports); and water and wastewater; usefully, regulations in several of these sectors already exist.

First, the North American Electric Reliability Council (which establishes regulations for the electric bulk transmission companies)[90] has recently promulgated new standards that, in substance, require the regulated companies to adopt a zero trust approach.[91] The standards include requirements for internal network monitoring,[92] configuration management,[93] universal multifactor authentication,[94] supply chain risk management,[95] and software provenance assurance.[96] Likewise, the Transportation Security Agency (TSA) has issued cybersecurity regulations[97] which cover rail,[98] aviation,[99] and pipelines[100] (including some recently proposed upgrades).[101] These cybersecurity requirements direct companies in the TSA-regulated sectors to adopt many zero trust requirements including:

- Network segmentation policies.
- Controls to ensure that operational technology systems can continue to safely operate if an information technology system has been compromised.
- Access control measures to secure and prevent unauthorized access to critical cyber systems.
- Continuous monitoring and detection policies.
- Timely application of security patches and updates on critical systems.102

In response to Salt Typhoon, the Federal Communications Commission (FCC) issued a declaratory ruling that existing law (CALEA Section 105)[103] "affirmatively requires telecommunications carriers to secure their networks from unlawful access or interception of communications."[104] According to the January 2025 ruling, "CALEA obligates carriers to *prevent* [unauthorized] interception of communications or access to call-identifying information," [105] although the precise contours of that obligation were not clarified.[106] In November 2025, the FCC changed course and rescinded the declaratory ruling, deeming it "unlawful and ineffective," but reiterated support for "[c]ollaboration with carriers, coupled with *targeted, legally robust regulatory and enforcement measures*..."[107] citing as an example the administration's new cybersecurity requirements for submarine cable licensees.[108]

As the foregoing suggests, critical infrastructures in some important sectors are not covered by federal cybersecurity standards. Those include electric generation and distribution, and water and wastewater, each of which is generally subject to state-level regulatory authorities. Given the critical importance of Section 9 companies to national and economic security, the administration and the Congress should each take steps to require enhanced cybersecurity for such nonregulated companies. Legislation should be enacted that would authorize the necessary regulations for each key sector not yet covered by federal legislation. While any such legislation could cover the entire sector, in keeping with the focus on the most important companies, the initial legislation should be limited to a sector's Section 9 companies. Historically, regulation of electric power generation and distribution and of water and wastewater has been done at the state level and there would be substantial political resistance to an entirely federal system. The importance of Section 9 companies to national and economic security, however, warrants cybersecurity regulation at the federal level.

An additional element of the proposed legislation would be to give the NCD the authority and obligation to harmonize cybersecurity requirements if a company is subject to more than a single set.[109] Concomitantly, the legislation should establish that companies will have a single regulatory point of contact with the government for required cybersecurity reviews.

ZTA Task Force

Section 9 companies will, of course, be able to choose from the full spectrum of the private sector in undertaking the implementation of zero trust. Given the importance of ensuring the highest degree of cybersecurity, however, an additional valuable resource should be created by the government by establishing a public-private team—a ZTA Task Force to work with Section 9 companies to implement the installation and operation of zero trust architectures.

A ZTA Task Force (like the Formal Methods Task Force) would consist of experts from the National Cyber Lab Cohort (i.e., experts from FFRDCs, UARCs, and the National Labs) and industry. The ZTA Task Force should have core members, complemented for each sector with sector experts. It would provide support to Section 9 companies for the transition of both IT and OT systems to ZTAs. Additionally, given the DoD's recently released ZTA guidance for OT, the task force should consult closely with the DoD leads for ZTA.

The expertise of the task force members will be important to ensure that the task force activities complement the many ongoing actions already being undertaken to enhance cybersecurity in key sectors.[110] It will be important for the ZTA Task Force to provide valuable functional support, but to avoid adding bureaucratic clutter. In this regard, and as noted above, the task force should be under a single construct along with the Formal Methods Task Force to assure effective coordination as well as integration of technological capabilities.

Technology road map: Advanced technology for ZTAs

Adversaries are, of course, seeking to defeat the very technologies utilized to establish an effective zero trust architecture. However, the development and use of advanced technologies can substantially increase the resilience of ZTAs. The ZTA Task Force should promote the use of each of the following:

- **Ephemeral authentication.** Ephemeral authentication reduces an organization's attack surface and minimizes risk by limiting the scope and duration of access. The key to ephemeral access is use of temporary credentials—such as certificates or tokens—to grant access to resources or systems. Ephemeral credential capabilities are available in the marketplace to be utilized in a zero-trust context. The credentials are created on-demand, expire quickly (after a set period) and automatically, and are discarded when they expire. In accordance with "just-in-time" access principles, ephemeral access ensures that users only have access when they need it and for the shortest time necessary, greatly limiting the window of opportunity for an attacker to exploit compromised credentials. Ephemeral access capabilities are not limited to verifying human users; they can likewise authenticate any entity connected to a network or a system, including computers and other devices.111 Just-in-time access "allows organizations to automatically grant, block, or revoke privileges based on current risk conditions without disrupting legitimate workflow."[112]
- **Quantum-resistant encryption.** Encryption can make adversarial intrusions seeking access to information ineffective as the adversary will not be able to read or review the encrypted data. Encryption needs to be utilized for both "data at rest" (maintained in a database) and "data in transit" (e.g., when moving from the cloud to a user). Multiple capabilities are available to provide such protection, including encryption products that incorporate quantum-resistant Federal Information Processing Standard-approved algorithms for data encryption, such as AES256 (one of the strongest block ciphers available) and ML-KEM (a lattice-based algorithm that can be used to establish a shared secret key between two parties communicating over a public channel).113 Notably, the private sector already is embracing such capabilities. Google, for example, recently updated the cryptography used in the Chrome browser to ML-KEM,114 and Microsoft has likewise updated its core cryptographic library with ML-KEM.115
- **Software segmentation.** Hardware and software segmentation of networks and systems are key elements of secure enterprise architectures. As CISA and other federal cybersecurity agencies have described:

> Through strict network segmentation and the enforcement of principles of least privilege, an organization could restrict the threat actor's ability to move laterally across the network. Even if high-level credentials are extracted, segmentation could limit the actor's reach to isolated network segments. Additionally, robust privileged access management would ensure that elevated access is granted sparingly and monitored closely, making it challenging for a cyber threat actor to misuse stolen credentials.[116]

DARPA is undertaking to further enhance segmentation's ability to limit the access an intruder may obtain.

DARPA's Compartmentalization and Privilege Management (CPM) program "aims to enhance cyber resilience by automatically subdividing software systems into smaller, secure compartments, preventing initial breaches from escalating into successful cyberattacks while maintaining system efficiency."[117]

The CPM program is still in its early days. Nonetheless, as the DARPA lead for the CPM has described, the required technology is available for application, with "the techniques for doing that actually [being] old AI techniques [and the] analysis part is based on what computer scientists call formal methods,"[118] with the latter being well-known, as discussed above.

- **Agentic AI.** Agentic cybersecurity involves artificial intelligence capabilities that can perform designated tasks (i.e., act as an agent) and are relatively recent developments. Agentic AI systems can make "independent decisions, adapt to new data, and execute complex tasks, setting them apart from standard AI."[119]

  One of the most effective applications of agentic AI in cybersecurity is autonomous threat detection and response.[120] AI-driven security systems can continuously monitor networks, identify suspicious patterns, and take immediate action, often faster than human analysts. An AI security agent, for example, can isolate compromised endpoints, block malicious IPs, and update firewall rules in real time to reduce the risk of breaches.[121] As one analysis described, AI-enabled agentic frameworks can reduce response time to address "vulnerabilities by investigating the risk of a new common vulnerability or exposure in just seconds. They can search external resources, evaluate environments and summarize and prioritize findings so human analysts can take swift, informed action.[122]"

  Microsoft's Project Ire malware detection prototype, for example, is powered by an autonomous AI agent specifically designed to analyze the structure and behavior of software.[123] Project Ire reported a 90 percent "catch rate" in early testing.[124]

  The importance of autonomous agents in dealing with such challenges is underscored by the massive scale of ongoing cyberattacks:

  Between January and December 2024, Microsoft detected more than 30 billion phishing emails targeting customers. The volume of these cyberattacks overwhelms security teams relying on manual processes and fragmented defenses, making it difficult to both triage malicious messages promptly and leverage data- driven insights for broader cyber risk management.[125]

  Agentic AI can add to cybersecurity for critical infrastructures. Inside the network, agentic AI can speed reaction times to intrusions. In doing so, however, it will be important to ensure that the responses do not inadvertently negatively affect the operation of the critical infrastructure. As one Nvidia analysis noted, "Agentic systems, by design, operate with significant autonomy, enabling them to perform impactful actions that can be both beneficial or potentially harmful."[126] Thus, extending agentic AI to OT systems "heightens the stakes, as compromises can directly impact uptime, safety and the integrity of physical operations."[127] Nonetheless, the potential benefit of agentic AI to cybersecurity for critical infrastructures warrants its further development and future usage in those situations where the benefits outweigh the risks. Moreover, as described above, formal methods should be utilized to ensure the appropriate working of the programs developed by agentic AI.

Regional resilience districts and ZTAs

As described in Part I of this report, Congress should authorize the establishment of regional resilience districts with a focus on mitigating regional cybersecurity risks across sectors.

The activities of the proposed regional resilience districts would be built around a registry identifying and prioritizing cyber risks. The regional risk registry would be developed in conjunction with private, state and local, and federal entities. Such a regional resilience district could then undertake cyber risk mitigation and responses through a combination of the capabilities of high-end cybersecurity providers (especially the ICPC companies discussed in the Part I companion report) and zero trust architectures with both the engaged critical infrastructures and with state and local governments. Such an arrangement could be particularly useful in dealing with cascading risks generated by cybersecurity attacks.

How to structure and distribute cybersecurity tax credits

The authors have previously proposed that Congress establish cybersecurity investment tax credits, advocating in 2022 that they be offered first to "innovative small and medium businesses and academia engaged in advancing selected emerging and advanced technologies" or to key critical infrastructures such as the electric grid, pipelines, water, and transportation. The scope would be up to Congress: "The amount of the credits could be equal to the price charged by the integrated cybersecurity provider." We saw and continue to see benefit in structuring the legislation to enable transferring unused tax credits to the cybersecurity service provider as "payment of the cost of the service."

Source: Franklin D. Kramer, Melanie J. Teplinsky, and Robert J. Butler, "We Need a Cybersecurity Paradigm Change," Opinion, Hill, February 15, 2022, https://thehill.com/opinion/cybersecurity/594296-we-need-a-cybersecurity-paradigm-change/.

The ZTA Task Force (described above) could play a key role in aiding both the design and implementation of the necessary zero trust architectures and in ensuring that relevant private-sector expertise was available to the membership of the regional resilience districts.

Additionally, as recommended in Part I, pilot programs for one or several port cities would be an excellent way to begin such an effort and would be of high consequence both for military reasons and for support to the public. Assuming the pilot efforts were successful, they could be expanded to other areas as steps toward more effective national resilience.

Financial support

As a key part of accomplishing zero trust for Section 9 companies as quickly as possible, the federal government should undertake to provide financial assistance. Cybersecurity is clearly a national security priority—as exemplified by the fact that the North Atlantic Treaty Organization's new defense spending goals will include cybersecurity as a recognized item.[128] Congress should undertake to define the level of spending that will be necessary to support ZTAs for Section 9 companies and then authorize and appropriate the amounts needed to put the required systems in place. Once ZTA is established for a company, upgrades and maintenance will be necessary. Congress could continue a system of direct support, or it might provide for a system of cybersecurity tax credits to help offset costs[129] or matching federal funds for state-funded initiatives.

While this report has identified numerous existing technological and architectural improvements that could bolster critical infrastructure cybersecurity, the rapid pace of change necessitates a set of organizational structures and repeatable processes that could be used to accelerate the development and adoption of future cyber "solutions." These include not only the structures and processes necessary to leverage cutting-edge private- and public-sector expertise for the benefit of critical infrastructure cybersecurity, but also the incentives (e.g., funding and liability protections) necessary to spur private-sector cooperation as well as the sustained multiyear funding necessary to retain and grow the research and development base essential to secure our most important critical infrastructures.

Making America's space enterprise safe and secure in cyberspace

Space systems are integral to making America safe and secure from adversary attacks. The Trump administration has asked for a "Golden Dome" capability that includes new space-based sensors; space-based missile interceptors; non-kinetic missile defense capabilities, such as electronic warfare tools; and military satellites with air moving target indicators. All of these space-based elements afford an opportunity for us to build cyber safe and secure systems using the approaches discussed above. Space Force, as the lead government developer, for many of these capabilities, can and should immediately adopt the system technologies and capabilities, enterprise architecture, and process improvements suggested in this paper.

As a start, Space Force should pilot these improvements in one of its critical Golden Dome support systems such as the Next Generation Overhead Persistent Infrared (Next-Gen OPIR) effort which is being developed as the replacement for the current missile warning constellation known as Space-Based Infrared System (SBIRS).

Integral to Next-Gen OPIR's success is a new, highly automated ground system called the Future Operationally Resilient Ground Evolution. FORGE has had developmental challenges that demand a new approach. Last year (2025,) Space Force changed the acquisition approach to allow the government to deliver capability in an agile, incremental and more modular way[172]. Building on these relatively recent changes, the FORGE Program Office could further strengthen the cyber resilience of this integrated enterprise by applying key technological advances for securing code bases (described above) and by moving to an AI-enabled, zero trust architecture which would support more rigorous and rapid testing of interconnected ground, airborne, and space-based systems. To remedy past problems of the legacy SBIRS ground command and control system and further ensure trust in this architecture, the FORGE system should use AI-enabled ephemeral authentication and encryption. Taking another step forward in both resilience and speed, FORGE prime contractors should partner with ICPC cybersecurity companies and develop an agentic cybersecurity framework for the entire ground system: AI bots would work together for collaborative sensing, collecting, and logging, and automatically characterize anomalies, fixing inherent software vulnerabilities and rapidly alerting of operationally introduced vulnerabilities.

To move in this direction with speed and scale, the Space Force—under the new AI-enabled DOD Software Fast Track authority—should seek rapid approvals for bots and systems to securely connect to the FORGE enterprise. From a contractual standpoint, this type of work could be incented through an "other transactional authority" contract, providing the contract team guaranteed work with limited liability protection as it seeks to significantly reduce technical risk and increase performance of the overall system.

Beyond these steps, Space Force should also pioneer cyber secure approaches for the critical infrastructure supporting FORGE system development, deployment, and maintenance. As an initial step, Space Force should seek to begin a dialogue with telecommunications, electric utility, and water utility owners at locations that are providing support to FORGE. System threat, proposed enterprise architectures, and the concept of operations should be shared with industry partners to ensure secure and reliable support for the life cycle of the FORGE system. Service level agreements should include the ability for AI-enabled systems to look beyond the fence line for software vulnerabilities being introduced by critical infrastructure operations and to provide mutual alerting for rapid remediation.

Sources: Ellen Mitchell, "5 Things to Know as Trump Rolls Out Golden Dome Missile Defense Shield, *Hill*, May 20, 2025, https://www.msn.com/en-us/news/politics/5-things-to-know-as-trump-rolls-out-golden-dome-missile-defense-shield/ar-AA1E96PE?ocid=BingNewsSerp; and see Theresa Hitchens, "Next-Gen OPIR: 2 Steps Forward, 1 Step Back for Missile Warning Effort," *Breaking Defense*, May 3, 2024, https://breakingdefense.com/2024/05/next-gen-opir-2-steps-forward-1-step-back-for-missile-warning-effort/.

IV. Conclusion

A national cybersecurity strategy will require not only an operational road map for offensive and defensive campaigning, but a technology road map which significantly enhances resilience for key critical infrastructures. This technology road map is built upon the development and adoption of safe coding and the implementation of zero trust architectures. Establishment of such capabilities will provide the president and the national leadership with the necessary capabilities to deter and defeat nation-state and criminal activities in cyberspace.

About the authors

Franklin D. Kramer is a distinguished fellow at the Atlantic Council and serves on its board. He is a former US assistant secretary of defense for international security affairs.

Robert J. Butler is a co-founder and the managing director of Cyber Strategies LLC. He served as the first deputy assistant secretary of defense for space and cyber policy and has also served as the chief security officer of a global data center company, among other corporate roles.

Melanie J. Teplinsky is an adjunct professor and senior fellow in the Technology, Law and Security Program at American University, Washington College of Law. She previously practiced technology law at Steptoe & Johnson LLP and served (pre-IPO) on the advisory board for CrowdStrike Inc.

Appendix: The cybersecurity challenge: Adversaries

A fundamental cybersecurity challenge facing the United States is that US information and operational technology systems are at high risk from state-sponsored attacks by China, Russia, Iran, and North Korea and from financial and other attacks by criminal organizations.

China

Perhaps most significantly, the People's Republic of China has penetrated critical operational infrastructures throughout the country. Jen Easterly, then-director of CISA, described in her blog how Volt Typhoon, a malicious state-sponsored cyber actor connected to the PRC, targeted critical US infrastructure. Easterly also cited praise from then-Rep. Mark E. Green, who stated on the House floor: "By prepositioning cyber threats within critical infrastructure networks, Volt Typhoon was poised to launch destructive cyberattacks of immense proportions against the U.S." Critical infrastructure organizations were compromised, he explained, but CISA had "detected and evicted" Volt Typhoon from many of them.[130]

Likewise of high concern was Salt Typhoon, a PRC state-sponsored cyber threat actor that reportedly targeted networks in more than eighty countries.[131] Salt Typhoon "breached at least nine U.S.-based telecommunications companies with the intent to target high profile government and political figures."[132]

More recently, China state-aligned hacking groups—including Linen Typhoon and Violet Typhoon[133]—have exploited vulnerabilities in Microsoft's SharePoint Server software to engage in a major cyber-espionage campaign affecting hundreds of agencies, businesses, and organizations. While the full extent of the SharePoint breach is not yet known (as of this writing, the investigation has only just begun), victims reportedly include the National Reconnaissance Office's Acquisition Research Center website,[134] the Department of Energy's National Nuclear Security Agency,[135] the Department of Homeland Security, and the Department of Health and Human Services including the National Institutes of Health.[136] Moreover, what started as a cyberespionage campaign now appears to have evolved, with Storm-2603—a China-based threat actor—having been observed exploiting the SharePoint vulnerabilities to deploy ransomware.[137]

Other high-profile Chinese attacks — including Operation Aurora,[138] the 2014 Office of Personnel Management hack,[139] the Equifax hack,[140] and the Microsoft Exchange/Hafnium hack[141]—have targeted valuable individual, business, and government information, including industrial trade secrets.

Russia

Russia has similarly undertaken highly significant cyberattacks: The Solar Winds supply chain attack affected almost 18,000 software clients,[142] the damages from the NotPetya attack exceeded $10 billion,[143] and the Viasat attack affected multiple commercial companies and communications throughout Europe.[144]

Iran

Iranian cyberattacks have long targeted US financial institutions and other critical infrastructure. A group of Iranian hackers working for an Iranian Revolutionary Guard Corps affiliate were indicted for infamous distributed denial of service attacks against dozens of US financial-sector victims that began in 2011.[145] One of those hackers was later charged with infiltrating the supervisory and control systems of the Bowman Dam in New York.[146] More recently, CISA and the US Department of Treasury have cited Iranian attacks "against operational technology devices,"[147] and using "ransomware attacks against critical infrastructure,"[148] respectively; it is notable that Iranian targeting of industrial control system devices also can enable espionage or disruptive or destructive attacks against critical infrastructures.[149]

North Korea

North Korea has a long history of engaging in cyberattacks including the well-known Sony[150] and Wanna Cry attacks.[151] Much of the North Korean cyber effort is undertaken to support its overall economic resilience, including through attacks on cryptocurrency,[152] and its nuclear program, including cyberespionage to obtain nuclear secrets and leveraging ransomware operations to finance its nuclear weapons program.[153] Notably, North Korea has attacked key critical infrastructures through, for example, ransomware campaigns targeting healthcare and public health organizations and other sectors.[154]

Criminal organizations

Multiple criminal organizations have undertaken frequent ransomware attacks[155] against vulnerable targets such as state and local governments and hospitals and other health providers.[156] Likewise, individual, business, and governmental information has regularly been stolen by criminal organizations—as exemplified by the attacks on national public data, resulting in the disclosure of millions of records containing personally identifiable information and the theft of valuable trade secrets.[157] Advanced artificial intelligence capabilities are expected to supercharge ransomware[158] and other criminal operations, with 80 percent of examined ransomware attacks already using AI, according to recent MIT Sloan research.[159] Not only are criminals increasingly using AI models to automate various stages of criminal operations (e.g., reconnaissance, credential harvesting, and network penetration)[160] in furtherance of sophisticated attacks,[161] but artificial intelligence also is lowering barriers to entry, allowing criminals with minimal technical skill to carry out complex cybercrime operations,[162] including against industrial control systems.[163]

The risks and losses from these ongoing cyber invasions are of enormous consequence to the United States. From a national security perspective, attacks against key infrastructures—such as the electric grid, railroads, or ports—during a conflict would significantly degrade the US capacity to achieve the country's war aims. As a recent report concluded, "The cybersecurity of the critical air, rail, and maritime infrastructure that underpins U.S. military mobility is insufficient."[164] There is, however, little doubt that an adversary—for example, China in the context of a Taiwan scenario or Russia in a European contingency—would undertake precisely such actions. As the March 2025 *Annual Threat Assessment of the U.S. Intelligence Community* states:

> If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision- making, inducing societal panic, and interfering with the deployment of U.S. forces.[165]

Regarding Russia, the assessment states:

> Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat. Moscow's unique strength is the practical experience it has gained integrating cyber attacks and operations with wartime military action, almost certainly amplifying its potential to focus combined impact on U.S. targets in time of conflict.[166]

The potential for significant impact on key critical infrastructures has been demonstrated in the context of the Russia-Ukraine war. According to *The Kyiv Independent*, Ukraine's military intelligence agency (known as HUR) inflicted damage in "a large-scale cyberattack against the network infrastructure of Russian energy giant Gazprom." Disruptions from the July 18 attack included:

> Hundreds of terabytes of data were downloaded by the Ukrainian hackers prior to their deletion from the Russian systems [and] . . . the attackers managed to destroy clusters of "extremely powerful" servers running 1C, a software widely used for managing documents and contracts, analytics data for pipelines, valves, pumps, and SCADA [supervisory control and data acquisition] systems—key elements in operating Gazprom's technical infrastructure. [Additionally], multiple servers reportedly had operating systems removed or disabled, and the BIOS (i.e., basic firmware) of many devices was damaged, making them inoperable without physical repairs.[167]

The harms from cyberattacks are not, however, confined to the national security sphere. Economic losses from cyberattacks are estimated to be in the hundreds of billions of dollars (some estimates are in the trillions[168]), with one estimate placing US economic losses at $320 billion for 2023.[169] A World Bank cybersecurity literature survey, while emphasizing the difficulty of determining the reliability of available data,[170] nonetheless concluded:

> Our analytical survey reveals that the economic losses of cyber incidents go beyond the immediate quantifiable costs since cyber incidents often incur indirect costs that have often remained unmeasured. For example, our survey reveals that cyber incidents can translate into systemic risk in financial markets, contagion effects to other firms in the same industry, and volatility in both domestic and global stock markets.[171]

In sum, for both national security and economic reasons, it is time—indeed, past time—for a far more effective approach to ensure the cybersecurity of the United States.

Endnotes

[1] Catalin Campanu, “Microsoft: 70 Percent of All Security Bugs Are Memory Safety Issues,” February 11, 2019, https://www.zdnet.com/article/microsoft-70-percent-of-all-security-bugs-are-memory-safety-issues/; Cyberthreat Intelligence Integration Center, “Recent Cyber Attacks on U.S. Infrastructure Underscore Vulnerability of Critical US Systems, November 2023 – April 2024,” https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf.

[2] The US Department of Homeland Security annually identifies and maintains a list of “Section 9 entities,” which are those critical infrastructure entities that meet the criteria specified in Executive Order 13636, Improving Critical Infrastructure Cybersecurity, Section 9(a). Section 9 entities are defined as «critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.» See “Support to Critical Infrastructure at Greatest Risk (“Section 9 Report”) Summary,” Cybersecurity and Infrastructure Security Agency (CISA), February 8, 2021, https://www.cisa.gov/resources-tools/resources/support-critical-infrastructure-greatest-risk-section-9-report-summary.

[3] Deirdre Doherty and Brian McKenney, “Zero Trust Architectures: Are We There Yet,” The MITRE Corporation, June 2021, https://www.mitre.org/sites/default/files/2021-12/pr-21-1273-zero-trust-architectures-are-we-there-yet.pdf.

[4] Memory-safety errors occur when “software, accidentally or intentionally, accesses system memory in a way that exceeds its allocated size and memory addresses,” Catalin Cimpanu wrote, adding, “Terms like buffer overflow, race condition, page fault, null pointer, stack exhaustion, heap exhaustion/corruption, use after free, or double free—all describe memory safety vulnerabilities.” See Cimpanu, “Microsoft: 70 Percent of All Security Bugs Are Memory Safety Issues,” *ZDNet*, February 11, 2019, https://www.zdnet.com/article/microsoft-70-percent-of-all-security-bugs-are-memory-safety-issues/.

[5] Bob Lord, “The Urgent Need for Memory Safety in Software Products,” CISA, revised December 06, 2023, https://www.cisa.gov/news-events/news/urgent-need-memory-safety-software-products. For a general discussion of the importance of memory safety in reducing software vulnerabilities, see NSA, CISA Joint Cybersecurity Information Sheet, “Memory Safe Languages: Reducing Vulnerabilities in Modern Software Development,” June 2025.

[6] Lord, “The Urgent Need.”

[7] “Memory Safety,” Android Open Source Project, last updated December 2, 2025, https://source.android.com/docs/security/test/memory-safety (“Memory safety bugs . . . are the most common issue in the Android codebases. They account for over 60 percent of high severity security vulnerabilities and for millions of user-visible crashes.”)

[8] Nicole Spewak, “Understanding Memory Safety Vulnerabilities: Top Memory Bugs and How to Address Them,” RunSafe Security, February 26, 2025, https://runsafesecurity.com/blog/memory-safety-vulnerabilities/.

[9] Spewak, “Understanding Memory Safety.”

[10] “Depending on the type of vulnerability, a malicious actor may be able to illicitly access data, corrupt data, or run arbitrary malicious code. For example, a malicious actor may send a carefully crafted payload to an application that corrupts the application’s memory, then causing it to run malware. Alternatively, a malicious actor may send a malformed image file that includes malware to create an interactive shell on the victim system. If an actor can execute arbitrary code in this way, the actor may gain control of the account running the software.” See “The Case for Memory Safe Roadmaps,” CISA, December 2023, 4, https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf.

[11] Trey Herr et al., “Buying Down Risk: Memory Safety,” Atlantic Council, May 3, 2022, https://www.atlanticcouncil.org/content-series/buying-down-risk/memory-safety/.

[12] NSA and CISA, “Memory Safe Languages: Reducing Vulnerabilities in Modern Software Development,” June 2025, https://media.defense.gov/2025/Jun/23/2003742198/-1/-1/0/CSI_MEMORY_SAFE_LANGUAGES_REDUCING_VULNERABILITIES_IN_MODERN_SOFTWARE_DEVELOPMENT.PDF

[13] K. D. Uttecht, “Zero Trust (ZT) Concepts for Federal Government Architectures,” Lincoln Laboratory, MIT, July 30, 2020, v, https://apps.dtic.mil/sti/pdfs/AD1108910.pdf.

[14] Francis Dinha, “How Zero Trust Could Have Changed the Outcome,” *Forbes*, April 4, 2022, https://www.forbes.com/councils/forbestechcouncil/2022/04/04/how-zero-trust-could-have-changed-the-outcome/.

[15] Gary Barlet, “Learnings from 3 Recent Cyberattacks Point to Zero Trust Segmentation,” Illumio blog, May 8, 2024, https://www.illumio.com/blog/learnings-from-3-recent-cyberattacks-point-to-zero-trust-segmentation.

[16] Barlet, “Learnings From 3 Recent Cyberattacks.”

[17] Cloud Security Alliance, “Zero Trust Guidance for Critical Infrastructure,” October 28, 2024, https://cloudsecurityalliance.org/artifacts/zero-trust-guidance-for-critical-infrastructure.

[18] North American Electric Reliability Corporation (NERC), “Zero Trust Security for Electric Operations Technology,” White Paper, June 2023, https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Zero_Trust_For_Electric_OT.pdf.

[19] Amit Pawar et al., *Navigating the 2025 NERC CIP Updates and Internal Network Security Monitoring (INSM) Requirements*, Xage Security, Itegriti, and LTIMindtree, https://info.xage.com/hubfs/Whitepapers_Guides_ebooks_Use%20Cases/Navigating%20the%202025%20NERC%20CIP%20Updates%20&%20INSM%20Requirements.pdf; Dragos Webinar, Manageable Zero Trust for OT Networks, February 5, 2021, https://www.youtube.com/watch?v=w1jHsR_yEhQ; and Fortinet, *A Solution Guide to Operational*

Technology Cybersecurity, https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-solution-guide-to-ot-cybersecurity.pdf.

20 Jim McCarthy et al., *Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity*, NIST Special Publication 1800-32B, iii, https://www.nccoe.nist.gov/sites/default/files/2022-02/es-iiot-nist-sp1800-32b-final.pdf.

21 McCarthy et al., *Securing Distributed Energy Resources*, 19–38.

22 Jim McCarthy et al., *Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry*, NIST Special Publication 1800-23, May 2020, 33–39, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-23.pdf.

23 Brandi Vincent, “DOD Putting Final Touches on New Zero Trust ‘Assessment Standard,’ ” *DefenseScoop*, September 10, 2024, https://defensescoop.com/2024/09/10/dod-zero-trust-assessment-standard-les-call-fed-talks/; and Joseph Clark, “DOD Cyber Officials Detail Progress on Zero Trust Framework Roadmap,” DOD News, April 3, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3729448/dod-cyber-officials-detail-progress-on-zero-trust-framework-roadmap/.

24 Mikayla Easley, DISA’s Thunderdome achieves advanced zero-trust goals, *DefenseScoop*, April 2, 2025, https://defensescoop.com/2025/04/02/disa-thunderdome-zero-trust-randy-resnick/

25 Mikayla Easley, Navy looks to add zero-trust controls into weapon systems, platforms, *DefenseScoop*, February 19, 2025, https://defensescoop.com/2025/02/19/navy-zero-trust-controls-ot-weapon-systems-platforms/#:~:text=Its%20cloud%2Dbased%20Microsoft%20Office,on%20other%20networks%2C%20Schumann%20noted.

26 O’Ryan Johnson, Dell’s Project Fort Zero Passes DoD Muster, *CRN*, April 4, 2025, https://www.crn.com/news/data-center/2025/dell-s-project-fort-zero-passes-dod-muster

27 DOD, Zero Trust for Operational Technology, November 18, 2025, https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OperationalTechnologyActivitiesOutcomes.pdf.

28 Grace Dille, “Army Official: DoD’s OT Guidance for Zero Trust Poses Major Challenge,” *MeriTalk*, March 19, 2025, https://www.meritalk.com/articles/army-official-dods-ot-guidance-for-zero-trust-poses-major-challenge/; Lisbeth Perez, “DoD Working on Zero Trust for OT Guidance Expected Summer 2025,” *MeriTalk*, December 11, 2024, https://www.meritalk.com/articles/dod-working-on-zero-trust-for-ot-guidance-expected-summer-2025/. The DOD Cybersecurity Reference Architecture describes ZTA analytically but does not provide an actual working architecture. DOD Zero Trust Reference Architecture, Version 2, July 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

29 Cloud Security Alliance, “Zero Trust Guidance for Critical Infrastructure,” October 28, 2024, 20, https://cloudsecurityalliance.org/artifacts/zero-trust-guidance-for-critical-infrastructure.

30 Richard Springer, “Is Zero Trust Right for OT, Right Now?” Fortinet, April 22, 2024, https://www.fortinet.com/blog/business-and-technology/is-zero-trust-right-for-ot.

31 “Demystifying Zero Trust in OT: Going from Implied Trust to Zero Trust,” Fortinet, July 24, 2023, https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-demystifying-zero-trust.pdf.

32 Jean-Pierre Joosting, “Formal Methods Are the Future of Embedded Software Verification,” eeNews Europe, July 31, 2025.

33 DARPA, “Formal Methods Examples,” https://www.darpa.mil/research/research-spotlights/formal-methods/examples. Caroline Guillaume, CEO of TrustInSoft, is quoted as saying, “Beyond memory safety, formal methods detect runtime errors like division by zero and integer overflows, which can cause unexpected program behaviour. They also verify that the code behaves as intended according to its specifications, ensuring functional correctness. Not only that, but formal methods help ensure adherence to coding standards . . . often required in safety-critical industries.” See Jean-Pierre Joosting’s interview with Guillaume, “Formal Methods Are the Future.”

34 DARPA, “Formal Methods Examples,” https://www.darpa.mil/research/research-spotlights/formal-methods/examples.

35 ISO 26262-1:2018, Road Vehicles – Functional Safety – Part 1: Vocabulary (recommending use of formal methods), https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-2:v1:en.

36 DO-178C, Software Considerations in Airborne Systems and Equipment Certification (this widely recognized standard for development of safety-critical software in the aerospace industry specifically includes guidance on the application of formal methods). “Safety Critical Software for Mission Critical Applications to Get Boost with Release of DO-178C,” *Military + Aerospace Electronics*, October 21, 2010, https://www.militaryaerospace.com/communications/article/16724089/safety-critical-software-for-mission-critical-applications-to-get-boost-with-release-of-do-178c.

37 ISO 13485, Medical Devices – Quality Management Systems – Requirements for Regulatory Purposes, 2016 (this standard aligns with the principles of formal methods although it does not mandate their use), https://www.iso.org/standard/59752.html.

38 International Atomic Energy Agency, *Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control*, Technical Report Series No. 384 (1999), https://www-pub.iaea.org/MTCD/Publications/PDF/TRS384_scr.pdf; “Formal Verification of Nuclear Systems: Past, Present and Future,” *Information & Security* 28, no. 2 (2012): 223–235, https://procon.bg/system/files/28.18_Lawford_Wassyng.pdf; and Andrew Shaughnessy, “How Do You Modernize Safety Critical Designs in Nuclear Power? RDE!,” Galois, September 13, 2024, https://www.galois.com/articles/how-do-you-modernize-safety-critical-designs-in-nuclear-power-rde.

39 Chris Newcombe et al., “How Amazon Web Services Uses Formal Methods,” *Communications of the ACM* 58, no. 4 (2015): 68, https://dl.acm.org/doi/pdf/10.1145/2699417.

40 Newcombe et al., “How Amazon Web Services Uses.”

[41] Newcombe et al., "How Amazon Web Services Uses."

[42] See Newcombe et al., "How Amazon Web Services Uses."

[43] Marc Brooker and Ankush Desai, "Systems Correctness Practices at Amazon Web Services: Leveraging Formal and Informal Methods," *Communications of the ACM* 68, no. 6 (2025): 38–42, ("surveying the portfolio of formal methods used across AWS"), https://cacm.acm.org/practice/systems-correctness-practices-at-amazon-web-services/.

[44] Brooker and Desai, "Systems Correctness Practices."

[45] Maurice H. Ter Beek et al., "Formal Methods in Industry," *ACM's Formal Aspects of Computing* 37, no. 1, Article 7 (December 2024), https://dl.acm.org/doi/pdf/10.1145/3689374.

[46] "In 2003, Astrée proved the absence of any runtime errors in the primary flight-control software of an Airbus model. The system's 132,000 lines of C code were analyzed completely automatically in only 80 minutes on a 2.8GHz 32-bit PC using 300MB of memory (and in only 50 minutes on an AMD Athlon 64 using 580MB of memory). Since then, Airbus France has been using Astrée in the development of safety-critical software for various plane series, including the A380." See also, "DARPA Guide for Formal Methods to Deliver Resilient Systems for Proposals," January 9, 2025, https://sam.gov/opp/127898f2979642eea65316c88a3169ba/view (explaining that "[a]irplane fly-by-wire control software is critical to the stability of the aircraft and is required to operate in real-time. Returning responses late is unacceptable. In 2003, the tool Astrée (see https://www.astree.ens.fr/) was able to prove that the C code of the Airbus A340 flyby-wire primary control system would never produce a run-time-exception and would always meet its real-time constraints.")

[47] Ter Beek et al., "Formal Methods in Industry,"

[48] "Cyber Technology R&D," BAE Systems, https://www.baesystems.com/en-us/product/cyber-r-d.

[49] Alastair Reid et al., "End-to-End Verification of ARM Processors with ISA-Formal," Proceedings of the 2016 International Conference on Computer Aided Verification, https://link.springer.com/chapter/10.1007/978-3-319-41540-6_3 (also available at https://alastairreid.github.io/papers/cav2016_isa_formal.pdf).

[50] Gerwin Klein et al., "Formally Verified Software in the Real World," *Communications of the ACM* 61, no. 10 (2018), https://cacm.acm.org/research/formally-verified-software-in-the-real-world/.

[51] Hanno Becker et al., "Combining Mechanized Proofs and Model-Based Testing in the Formal Analysis of a Hypervisor," Conference Paper in *FM 2016: Formal Methods*, eds. J. Fitzgerald et al., FM 2016, Lecture Notes in Computer Science 9995 (2016), Springer, Cham, https://doi.org/10.1007/978-3-319-48989-6_5 (and also accessible at https://friedhofsspaziergang-leipzig.de/papers/fireeye.pdf).

[52] J ohn Harrison, "Formal Methods at Intel – An Overview," *Second NASA Formal Methods Symposium*, April 14, 2010, https://shemesh.larc.nasa.gov/NFM2010/talks/harrison.pdf; also see https://ntrs.nasa.gov/api/citations/20100018529/downloads/20100018529.pdf; and https://ntrs.nasa.gov/api/citations/20100018535/downloads/20100018535.pdf.

[53] Nikolaj Bjørner, "Formal Methods at Microsoft," TLA+ Conference, September 22, 2022, https://conf.tlapl.us/2022/FormalMethodsAtMicrosoftNikolajBjornerTLAConference2022.pdf; and "Practical High Performance Verification in Rust," Microsoft, https://www.microsoft.com/en-us/research/project/practical-system-verification/.

[54] David Basin et al., "It Takes a Village: Bridging the Gaps Between Current and Formal Specifications for Protocols," *Communications of the ACM* 68, no. 8 (2025): 54, https://dl.acm.org/doi/pdf/10.1145/3706572.

[55] Basin et al., "It Takes a Village."

[56] David Basin, Ralf Sasse, and Jorje Toro-Pozo, "The EMV Standard: Break, Fix, Verify," *2021 IEEE Symposium on Security and* Privacy, May 2021, https://ieeexplore.ieee.org/document/9519404.

[57] Here, correctness means that a set of facts about a program's behavior is true, given a set of assumptions.

[58] Formal methods have been used to ensure, for example, that critical software used to build highly secure systems in sectors such as aerospace and defense (e.g., the seL4 microkernel) will never crash or perform an unsafe operation and will behave predictably in every situation. See Gerwin Klein et al., "seL4: Formal Verification of an Operating-System Kernel," *Communications of the ACM* 53, no. 6 (2010), https://dl.acm.org/doi/pdf/10.1145/1743546.1743574; Ter Beek et al., "Formal Methods in Industry"; "What Is seL4? A High-Assurance, High-Performance Operating System Microkernel," seL4, https://sel4.systems/About/; and DARPA, "Formal Methods Examples," https://www.darpa.mil/research/research-spotlights/formal-methods/examples. See also "The CompCert C Compiler," https://compcert.org/compcert-C.html (the CompCert C compiler used to compile safety- and mission-critical software has been formally verified, ensuring that compiled code behaves exactly as specified by the "formal semantics" of the C source code).

[59] DARPA, HACMS: High-Assurance Cyber Military Systems,https://www.darpa.mil/news/resources/case-studies/hacms; Yakoub Nemouchi, Sriharsha Etigowni, Alexander Zolan, Richard Macwan, Formally Verified ZTA Requirements for OT/ICS Environments with Isabelle/HOL: Preprint (October 2023), https://research-hub.nrel.gov/en/publications/formally-verified-zta-requirements-for-otics-environments-with-is (describing "a methodology and a framework for the system level verification of zero trust architecture requirements in operational technology environments").

[60] https://www.darpa.mil/research/programs/verified-security-and-performance-enhancement-of-large-legacy-software

[61] https://www.darpa.mil/research/programs/verified-security-and-performance-enhancement-of-large-legacy-software

[62] https://www.darpa.mil/research/programs/verified-security-and-performance-enhancement-of-large-legacy-software

[63] https://www.darpa.mil/research/programs/verified-security-and-performance-enhancement-of-large-legacy-software

64 https://www.nationaldefensemagazine.org/articles/2025/2/19/darpa-gets-word-out-on-secure-software-for-military

65 https://www.darpa.mil/research/programs/pipelined-reasoning-of-verifiers-enabling-robust-systems

66 https://www.darpa.mil/research/programs/pipelined-reasoning-of-verifiers-enabling-robust-systems

67 https://cacm.acm.org/practice/systems-correctness-practices-at-amazon-web-services/.

68 https://www.microsoft.com/en-us/research/project/practical-system-verification/; also see https://www.microsoft.com/en-us/research/publication/automated-proof-generation-for-rust-code-via-self-evolution/.

69 https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf [9]

70 https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf [9]

71 https://www.atlanticcouncil.org/content-series/buying-down-risk/memory-safety/

72 https://security.googleblog.com/2024/09/deploying-rust-in-existing-firmware.html

73 Jeff Vander Stoep and Alex Rebert, "Eliminating Memory Safety Vulnerabilities at the Source," Google blog, September 25, 2024.

74 See page 9 at https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf.

75 https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf

76 TRACTOR is short for "Translating All C To Rust."

77 https://www.darpa.mil/research/programs/translating-all-c-to-rust

78 https://www.darpa.mil/research/programs/translating-all-c-to-rust

79 https://devops.com/darpa-turns-to-ai-to-help-turn-c-and-c-code-into-rust/#:~:text=DARPA%2C%20the%20Defense%20Department's%20(DOD,adopt%20memory%2Dsafe%20programming%20languages

80 A CRS is a fully autonomous system that takes complete responsibility for defending a set of software services; see Thanassis Avgerinos et al., "The Mayhem Cyber Reasoning System," IEEE Computer and Reliability Societies, March/April 2018, 52.

81 https://aicyberchallenge.com/overview/

82 Per an Atlantic Council report, "OSS is code published under a license that allows anyone to inspect, modify, and re-distribute the source code. This helps developers share and re-use solutions to common problems, creating such efficiencies that some estimate that 97 percent of software depends on OSS. OSS ranges from small components for illustrating graphs to entire operating systems. Contributors include individuals working in their free time, staff at large companies, foundations, and many others. The ecosystem is community-based, with many governance structures to manage contributions and maintenance." See "Avoiding the Success Trap: Toward Policy for Open-source Software as Infrastructure," Atlantic Council Cyber Statecraft Initiative, February 2023, 2.

83 https://www.darpa.mil/news/2025/aixcc-results

84 https://www.darpa.mil/news/2025/aixcc-results

85 Kent Walker, "A Summer of Security: Empowering Cyber Defenders with AI," Google blog, July 15, 2025, https://blog.google/technology/safety-security/cybersecurity-updates-summer-2025/.

86 https://blog.google/technology/safety-security/cybersecurity-updates-summer-2025/.

87 Department of Justice, "Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers," Press Release, January 14, 2025, https://www.justice.gov/archives/opa/pr/justice-department-and-fbi-conduct-international-operation-delete-malware-used-china-backed.

88 The existing patchwork quilt of cyber regulations, including cyber incident reporting requirements, offers a cautionary tale with respect to harmonization. See, e.g., a US GAO letter to Senate Comm. on Homeland Security and Governmental Affairs, "Cybersecurity Regulations: Industry Perspectives on Impact, Progress, Challenges, and Opportunities of Harmonization," July 30, 2025, https://www.gao.gov/assets/890/880583.pdf; it lists negative impacts on industry of multiple and varying cybersecurity regulations. See also that committee's hearing titled "Regulatory Harm or Harmonization?," video, March 11, 2025, https://homeland.house.gov/hearing/regulatory-harm-or-harmonization-examining-the-opportunity-to-improve-the-cyber-regulatory-regime/.

89 Hearings Before the Senate Comm. on Homeland Security and Governmental Affairs, 118th Cong. (2024) (statement of David B. Hinchman, director of information technology and cybersecurity, GAO), https://www.gao.gov/assets/gao-24-107602.pdf.

90 Industrial Defender, "What Is NERC CIP: The Ultimate Guide," July 26, 2025, https://www.industrialdefender.com/blog/what-is-nerc-cip#latest.

91 See NERC, "Quick Reference Guide: Security Integration," January 2025, https://www.nerc.com/pa/Documents/Security_Integration__Quick%20Reference%20Guide.pdf. While NERC does not explicitly mandate zero trust, NERC encourages a zero trust approach to meet CIP standards. See also Xage Security White Paper, "Navigating the 2025 NERC CIP Updates and Internal Network Security Monitoring (INSM) Requirements," 2, https://info.xage.com/hubfs/Whitepapers_Guides_ebooks_Use%20Cases/Navigating%20the%202025%20NERC%20CIP%20Updates%20&%20INSM%20Requirements.pdf.

92 Rule Notice, Federal Energy Regulatory Commission: Critical Infrastructure Protection Reliability Standard CIP-015-1-Cyber Security-Internal Network Security Monitoring, 18 C.F.R. Part 40 (2025), https://www.federalregister.gov/documents/2025/07/02/2025-12309/critical-infrastructure-protection-reliability-standard-cip-015-1-cyber-security-internal-network.

[93] See, e.g., NERC CIP-010-4, effective October 1, 2022, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-4.pdf.

[94] See, e.g., NERC CIP-005-07 (requiring multifactor authentication for all interactive remote access to an electronic security perimeter environment for medium- and high-impact bulk electric power cyber systems), https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-7.pdf; approved by FERC, 174 FERC ¶ 61,193 (2021); see also NERC CIP-005-8, which was filed with FERC in 2024 and is pending regulatory approval, https://www.nerc.com/globalassets/standards/reliability-standards/cip/cip-005-8.pdf.

[95] See, e.g., NERC CIP-005-6, CIP-010-3, and CIP-013-1 (NERC supply chain risk management (SCRM) standards approved by FERC in 2018); see also NERC, 182 FERC ¶ 61,155 (2023) (approving new SCRM requirements for low-impact bulk electric system cyber systems). See also notice of proposed rulemaking (NPRM), Supply Chain Risk Management Reliability Standards, 89 Fed. Reg. 79794 (2024) (proposing to direct NERC to develop new/updated reliability standards to address the sufficiency of SCRM plans).

[96] See NERC CIP-013-2 (effective October 1, 2022); see also NERC Security Guideline: Supply Chain Provenance, March 22, 2023, (nonbinding guidelines reflecting collective industry experience).

[97] Hearing Before the House of Representatives Homeland Security Subcomm. on Transportation and Maritime Security, 118th Cong. (2024) (statement of Chad Gorman, deputy executive assistant administrator for operations support, Transportation Security Administration), https://www.congress.gov/118/meeting/house/117716/witnesses/HHRG-118-HM07-Wstate-GormanC-20241119.pdf.

[98] TSA rail security directives are listed in Table 1of the DHS Ratification of Security Directives, 90 Fed. Reg. 6777 (2025), https://www.govinfo.gov/content/pkg/FR-2025-01-21/pdf/2025-01422.pdf.

[99] Joint EA 23-01 (Cybersecurity-Performance-Based Measures) is not publicly available as it is considered “sensitive security information” under 49 C.F.R. § 1520.5(b). According to TSA, the aviation security requirements set forth in Joint EA 23-01 are similar to the performance-based requirements TSA previously issued to critical pipelines and rail entities. See TSA news release, March 7, 2023, https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-for-airport-and-aircraft.

[100] TSA security directives for critical pipeline systems are listed in Table 1 of the DHS Ratification of Security Directives, 90 Fed. Reg. 5491 (2025), https://www.govinfo.gov/content/pkg/FR-2025-01-17/pdf/2025-01243.pdf. See also, TSA, “Enhancing Pipeline Security Information Circular,” February 16, 2022, https://www.tsa.gov/sites/default/files/TSA%20Information%20Circular%20Pipeline-2022-01%20Package.pdf.

[101] See, e.g., TSA NPRM, Enhancing Surface Cyber Risk Management, November 2024, https://www.govinfo.gov/content/pkg/FR-2024-11-07/pdf/2024-24704.pdf.

[102] Jay Willoughby, “Preparing for TSA Cybersecurity Compliance with Identity Security,” Cyberark blog, July 18, 2023, https://www.cyberark.com/resources/blog/preparing-for-tsa-cybersecurity-compliance-with-identity-security.

[103] See Communications Assistance for Law Enforcement Act (“CALEA”), § 105.

[104] FCC Declaratory Ruling and Notice of Proposed Rulemaking, FCC 25-9 (2025), 8.

[105] FCC Declaratory Ruling and Notice of Proposed Rulemaking, FCC 25-9 (2025), 9 (emphasis added).

[106] FCC Declaratory Ruling and Notice of Proposed Rulemaking, FCC 25-9 (2025), 10.

[107] FCC, “Order on Reconsideration,” Protecting the Nation’s Communications Systems from Cybersecurity Threats, PS Docket No. 22-239, FCC 25-81, November 21, 2025 (emphasis added), https://docs.fcc.gov/public/attachments/FCC-25-81A1.pdf.

[108] FCC Press Release, “FCC Corrects Course, Outlines Improved Cybersecurity Measures,” November 20, 2025, https://docs.fcc.gov/public/attachments/DOC-415455A1.pdf.

[109] Regarding the need for cyber regulatory harmonization, see Sydney M. White and Kathleen E. Scott, “Cyber Regulatory Harmonization: The Prospects and Potential Impacts of Current Efforts,” Wiley blog, August 8, 2025, https://www.wileyconnect.com/Cyber-Regulatory-Harmonization-The-Prospects-and-Potential-Impacts-of-Current-Efforts. Indeed, as that Wiley blog points out, “The harmonization of cybersecurity incident reporting requirements was a key bipartisan driver of the Cybersecurity Incident Reporting for Critical Infrastructure Act.”

[110] As one example of the high degree of ongoing activity, a recent report focused on the energy sector described a “broad array of collaborative cybersecurity efforts between [state public utility commissions (PUCs)], DOE, national laboratories and universities, and industry partners. . . . including the Clean Energy Cybersecurity Accelerator, the Energy Cyber Sense program, and (in 2024 alone) sixteen new cybersecurity research and development efforts across six states.” See Paul Stockton, “Surfing the Wave: Resilience Strategies for the Decentralizing Grid,” Johns Hopkins Applied Physics Laboratory, 2025, 9, https://www.jhuapl.edu/sites/default/files/2025-03/SurfingTheWave-WEB.pdf.

[111] Apono, “What is Ephemeral Access?,” https://www.apono.io/wiki/ephemeral-certificates-ephemeral-access/; and CloudFlare, “What Is an Identity Provider?,” https://www.cloudflare.com/learning/access-management/what-is-an-identity-provider/.

[112] Steve McDowell, “CrowdStrike’s New Just-In-Time Approach to Privileged Access Management,” *Forbes*, April 23, 2025, https://www.forbes.com/sites/stevemcdowell/2025/04/23/crowdstrikes-new-just-in-time-approach--to-privileged-access-management/.

[113] The Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) Standard, FIPS 203, is the primary quantum-resistant standard for general encryption. See NIST, ML-KEM, August 13, 2024, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf.

[114] Bill Toulas, “Chrome Switching to NIST-Approved ML-KEM Quantum Encryption,” *Bleeping Computer*, September 16, 2024, https://www.bleepingcomputer.com/news/security/chrome-switching-to-nist-approved-ml-kem-quantum-encryption/; and Google Cloud, “Post-quantum Cryptography,” https://cloud.google.com/security/resources/post-quantum-cryptography (announcing that Google “has implemented ML-KEM in [its] cryptography library, BoringSSL, which allows for it to be deployed and utilized by services that depend on this library).

115 See Aahba Thipsay, "Microsoft's Quantum Resistant Cryptography Is Here," *Microsoft Security Community Blog*, September 9, 2024, https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsofts-quantum-resistant-cryptography-is-here/4238780; and SymCrypt, Microsoft's cryptographic library, https://github.com/microsoft/SymCrypt.

116 CISA et al., "Identifying and Mitigating Living Off the Land Techniques," Joint Guidance with US and allied agencies, February 7, 2024, 24, https://www.cisa.gov/sites/default/files/2025-03/Joint-Guidance-Identifying-and-Mitigating-LOTL508.pdf.

117 "DARPA Taps RTX to Strengthen Cyber Resiliency," RTX, November 7, 2024, https://www.rtx.com/news/news-center/2024/11/07/darpa-taps-rtx-to-strengthen-cyber-resiliency.

118 Tom Temin, "DARPA Tries a Simple but Profound Concept to Improve Cybersecurity," Federal News Network, November 22, 2024, https://federalnewsnetwork.com/cybersecurity/2024/11/darpa-tries-a-simple-but-profound-concept-to-improve-cybersecurity/#:~:text=DARPA%20tries%20a%20simple%20but%20profound%20concept%20to%20improve%20cybersecurity,-%5Bhbidc-podcast%20podcastid%3D'&text=The%20Defense%20Advanced%20Research%20Project,hard%20for%20hackers%20to%20access.

119 Theodoros Karasavvas, "How Agentic AI Is Transforming Enterprise Software Development and Cybersecurity," *LevelBlue Blog*, March 3, 2025, https://levelblue.com/blogs/security-essentials/how-agentic-ai-is-transforming-enterprise-software-development-and-cybersecurity. As the *Harvard Business Review* stated: "To achieve this level of autonomous decision-making and action, agentic AI relies on a complex ensemble of different machine learning, natural language processing, and automation technologies. While agentic AI systems harness the creative abilities of generative AI models such as ChatGPT, they differ in several ways. First, they are focused on making decisions rather than on creating content. Second, they do not rely on human prompts, but rather are set to optimize particular goals or objectives, such as maximizing sales, customer satisfaction scores, or efficiency in supply-chain processes. And third, unlike generative AI, they can also carry out complex sequences of activities, independently searching databases or triggering workflows to complete activities. See Mark Purdy, "What Is Agentic AI and How Will It Change Work?," *Harvard Business* Review, December 12, 2024, https://hbr.org/2024/12/what-is-agentic-ai-and-how-will-it-change-work.

120 US Cyber Command already is using AI tools to reduce the time it takes to analyze network traffic for malicious activity, according to Executive Director Morgan Adamski. See Derek B. Johnson, "Cyber Command Touts AI-Driven Gains In Cybersecurity, Network Monitoring," *CyberScoop*, April 2, 2025, https://cyberscoop.com/cyber-command-ai-gains-cybersecurity-network-monitoring/#:~:text=Executive%20Director%20Morgan%20Adamski%20said%20the%20agency's,days%20and%20weeks%20to%20hours%20and%20minutes.&text=Adamski%20said%20an%20AI%20task%20force%20in,other%20AI%20technologies%20into%20Cyber%20Command%20operations.

121 Karasavvas, "How Agentic AI Is Transforming."

122 See David Reber Jr., "How Agentic AI Enables the Next Leap in Cybersecurity" *Nvidia blog*, April 28, 2025, https://blogs.nvidia.com/blog/agentic-ai-cybersecurity/.

123 Brian Caswell et al., "Project Ire Autonomously Identifies Malware at Scale," Microsoft blog, August 5, 2025, https://www.microsoft.com/en-us/research/blog/project-ire-autonomously-identifies-malware-at-scale/.

124 Rabia Noureen, "Microsoft Launches Project Ire to Enhance Real-Time Threat Detection," Petri, August 19, 2025, https://petri.com/microsoft-project-ire-threat-detection/.

125 Vasu Jakkal, "Microsoft Unveils Microsoft Security Co-Pilot Agents and New Protections for AI," *Microsoft Security* blog, March 24, 2025, https://www.microsoft.com/en-us/security/blog/2025/03/24/microsoft-unveils-microsoft-security-copilot-agents-and-new-protections-for-ai/.

126 Reber Jr., "How Agentic AI Enables."

127 Reber Jr., "How Agentic AI Enables."

128 NATO, "The Hague Summit Declaration," June 25, 2025, https://www.nato.int/cps/en/natohq/official_texts_236705.htm; and "Experts React: NATO Allies Agreed to a 5 Percent Defense Spending Target in a Low-Drama Summit. Now What?," *New Atlanticist*, Atlantic Council blog, June 25, 2025, https://www.atlanticcouncil.org/blogs/new-atlanticist/experts-react/nato-allies-agreed-to-a-5-percent-defense-spending-target-in-a-low-drama-summit-now-what/.

129 Franklin D. Kramer, Melanie J. Teplinsky, and Robert J. Butler, "We Need a Cybersecurity Paradigm Change," Opinion, *Hill*, February 15, 2022, https://thehill.com/opinion/cybersecurity/594296-we-need-a-cybersecurity-paradigm-change/.

130 https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats

131 Adam Goldman, "'Unrestrained' Chinese Cyberattackers May Have Stolen Data from Almost Every American," *New York Times*, September 4, 2025.

132 Scott Caveza, "Salt Typhoon: An Analysis of Vulnerabilities Exploited by this State-Sponsored Actor," Tenable blog, January 23, 2025; Joint Cybersecurity Advisory, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," September 2025; and Davina Tham's report saying "the US Government has reportedly linked Salt Typhoon to China's Ministry of State Security," in "Singapore Actively Dealing with Ongoing Cyberattack on Critical Infrastructure: Shanmugam," CNA, July 18, 2025, https://www.channelnewsasia.com/singapore/unc3886-cyber-security-threat-actor-attack-singapore-5245791.

133 Microsoft assesses with "moderate confidence" that Storm-2603 is a China-based threat actor; see, "Disrupting Active Exploitation of On-premises SharePoint Vulnerabilities," updated July 23, 2025.

134 https://www.washingtontimes.com/news/2025/jul/24/major-intelligence-website-hacked-search-cia-spying-secrets/

135 Kristina Beek, "US Nuclear Agency Hacked in Microsoft SharePoint Frenzy," *DarkReading,* July 23, 2025, https://www.darkreading.com/cyberattacks-data-breaches/us-nuclear-agency-hacked-microsoft-sharepoint.

136 https://www.washingtonpost.com/technology/2025/07/23/sharepoint-microsoft-hack-nih-nnsa/; and https://www.nextgov.com/cybersecurity/2025/07/dhs-impacted-hack-microsoft-sharepoint-products-people-familiar-say/406941/.

137 Microsoft Threat Intelligence, "Disrupting Active Exploitation."

138 https://medium.com/kopfkino/operation-aurora-the-largest-cyber-heist-in-history-6da33219b121.

139 https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

140 https://medium.com/@shajalapsdel/inside-the-equifax-breach-a-case-study-on-what-went-wrong-84c4edf50536

141 https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/HAFNIUM%20Compromises%20MS%20Exchange%20Servers.pdf

142 https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

143 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

144 https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion

145 https://www.justice.gov/archives/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

146 https://www.justice.gov/archives/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

147 https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran

148 https://home.treasury.gov/news/press-releases/jy2292

149 https://www.wired.com/story/iran-apt33-industrial-control-systems/

150 https://www.fbi.gov/news/press-releases/update-on-sony-investigation

151 https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537

152 https://www.bbc.com/news/articles/c2kgndwwd7lo; https://cointab.com/how-lazarus-group-is-terrorizing-crypto/

153 https://www.csis.org/analysis/how-are-cyberattacks-fueling-north-koreas-nuclear-ambitions.

154 https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea; and https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

155 https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-examples/

156 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware; and https://securityintelligence.com/news/research-finds-56-percent-increase-active-ransomware-groups/.

157 Regarding the 2024 National Public Data breach exposing "up to 2.9 billion records with highly sensitive personal data of up to 170 million people in the US, UK and Canada," see, e.g., https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535.

158 The world's first "generative AI-powered ransomware implant" already is under development, https://www.infosecurity-magazine.com/news/first-ai-powered-ransomware/.

159 "Rethinking the Cybersecurity Arms Race: When 80% of Ransomware Attacks are AI Driven," Cybersecurity at MIT Sloan.

160 See, e.g., "Detecting and Countering Misuse of AI," Anthropic blog, August 2025, which describes how a sophisticated cybercriminal "used Claude Code to commit large-scale theft and extortion of personal data."

161 One cybercriminal, for example, "used Claude to develop, market, and distribute several variants of ransomware, each with advanced evasion capabilities, encryption, and anti-recovery mechanisms. The ransomware packages were sold on internet forums to other cybercriminals for $400 to $1,200 USD."

162 "Criminals with few technical skills are using AI to conduct complex operations, such as developing ransomware, that would previously have required years of training"; see "Detecting and Countering Misuse of AI," Anthropic blog, August 2025.

163 "Low-barrier tools like large language models (LLMs) and agentic AI platforms are transforming the cyber threat landscape by enabling 'script kiddies' and non-state actors to automate, scale, and iterate attacks against industrial control systems. The convergence of unsophisticated actors with powerful AI tools widens the attack surface for critical infrastructure while complicating attribution and defense." See Daniel Pereira, "A New Wave of Cyberattackers Enabled by Adversarial Use of LLMs and Agentic AI," *OODA Loop,* May 9, 2025.

164 See page 4 of a Foundation for Defense of Democracies monograph: https://www.fdd.org/analysis/2025/03/27/military-mobility-depends-on-secure-critical-infrastructure/.

165 See page 11 of the *US Annual Threat Assessment of the U.S. Intelligence Community*: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

166 See page 19 of *US Annual Threat Assessment of the U.S. Intelligence Community*: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

167 https://kyivindependent.com/ukrainian-intel-hackers-hit-gazproms-network-infrastructure-sources-say-07-2025/

168 https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/

169 https://ciphertex.com/2024/05/24/the-cost-of-cyber-theft-to-the-u-s-economy-in-2024/#:~:text=The%20Financial%20Impact&text=This%20figure%20includes%20expenses%20related,%E2%80%8B%20(Astra%20Security)%E2%80%8B

170 The breadth of estimates, ranging from the billions to the trillions, is reflected in a story from *The Economist*: “Nevertheless, it is clear that the scale is staggering, with billions, possibly trillions, of dollars in economic costs each year. The low end of the range comes from tallies of reported crimes by law-enforcement agencies. The FBI said it received reports of direct losses of $16.6bn in 2024, a 33% increase over 2023. Adding in unreported losses and wider economic costs leads to bigger numbers. Britain puts its current annual losses at more than £27bn (based on old data). The European Commission reckons that the worldwide costs of cybercrime were €5.5trn ($6.5trn) in 2021.” Separately, a top US national security official warned in 2023 that the global cost of cybercrime is projected to reach $23 trillion by 2027, per a US State Department digital press briefing.

171 See the conclusion in «A Review of the Economic Costs of Cyber Incidents,” World Bank, 13, https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf.

172 Space Force FORGEing ahead with missile warning ground system - Breaking Defense

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org