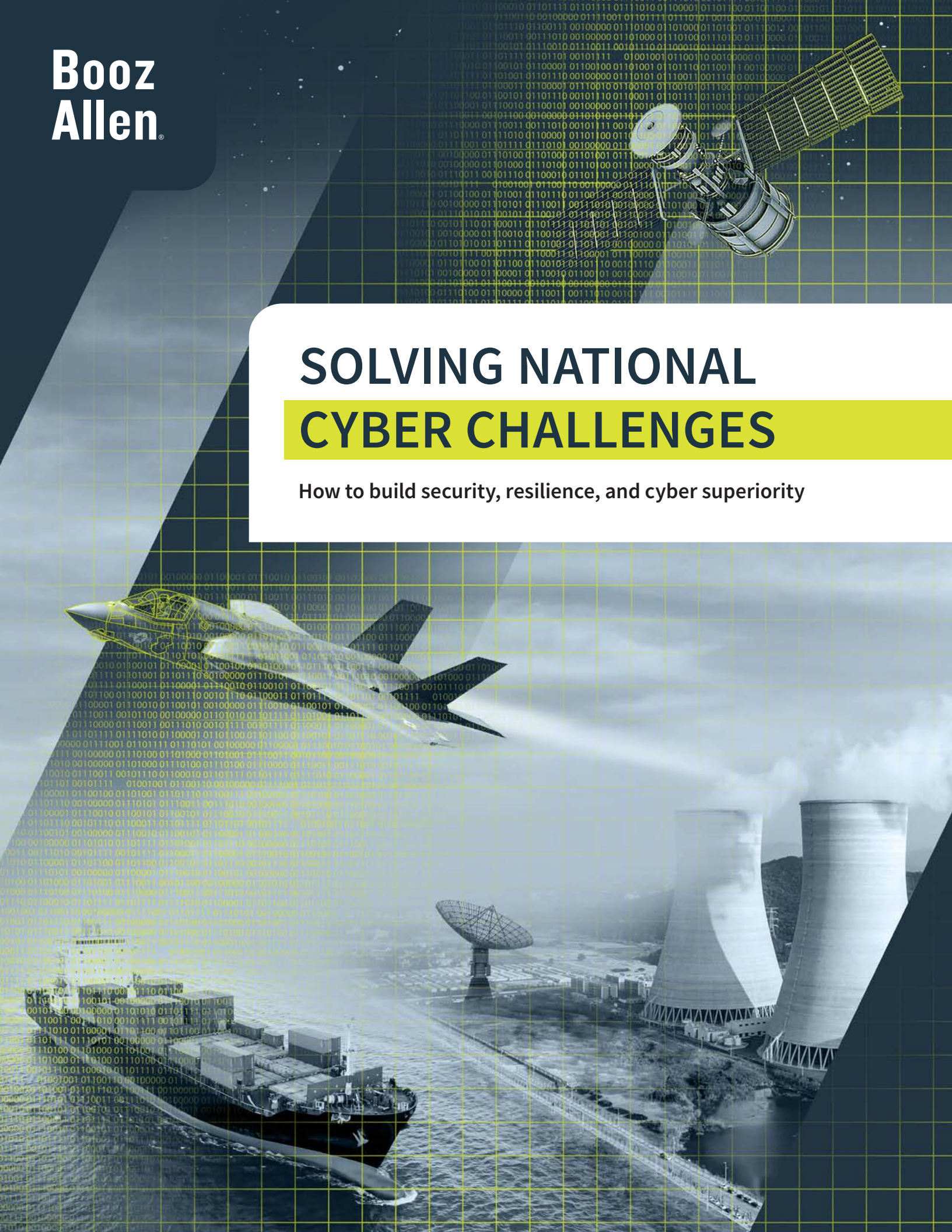
Booz Allen®

SOLVING NATIONAL CYBER CHALLENGES

How to build security, resilience, and cyber superiority



FOREWORD

Tomorrow's cyber threats will likely eclipse yesterday's.

That's why the **National Security Strategy** calls for decisive action to protect vital national functions and critical infrastructure—and it's why the **National Cybersecurity Strategy** doubles down on disrupting and dismantling threat activities. Adversaries view the federal government, intelligence agencies, the military, and all critical infrastructure industries as one large target-rich environment—one cyber battlespace.

To prevail and outpace adversaries, the United States must now employ cyber offense and defense in a seamless manner. What's needed is not just security and resilience but also cyber superiority.

The time to act is now. Cyber conflict is being waged in the shadows—but the danger is clear enough. Digital cloak-and-dagger operations, fueled by rising geopolitical tensions, threaten to undermine trusted IT systems, connected devices, and operational technology (OT), potentially causing physical effects.

But these urgent cyber challenges also present significant opportunities to advance the security, defense, and prosperity of the nation. On a grand scale, the United States, allies, partners, and the private sector can build unity of effort on three fronts:

- Fostering operational collaboration
- Focusing innovation
- Integrating cyber offense and defense capabilities with other tools of national power to deter and counter threats

What's more, organizations can immediately take steps to achieve measurable progress in these areas:

- Reducing systemic risk by outpacing threats to operational technology and industrial control systems (OT/ICS) in critical infrastructure sectors
- Protecting data and networks across government and industry by putting zero trust into practice
- Strengthening national defense by achieving decision advantage, accelerating the integration of cyber capabilities in special operations forces (SOF) training, and developing truly integrated cyber weapons

To help leaders across government, the intelligence community, the military, and the private sector seize these significant opportunities to sustain U.S. cyber superiority, we've assembled the enclosed insights and actionable advice.

CONTENTS

HOW TO SUSTAIN U.S. CYBER SUPERIORITY

Harness collaboration, innovation, offense, and defense

Tomorrow's cyber threats will likely eclipse yesterday's. That's why the 2022 **National Security Strategy** calls for decisive action to protect vital national functions and critical infrastructure—and it's why the **National Cybersecurity Strategy** doubles down on disrupting and dismantling threat activities. To prevail and outpace adversaries, the United States must now employ cyber offense and defense in a seamless manner. What's needed is not just security and resilience, but also cyber superiority.

Neither nations nor organizations can afford to wait for a catastrophic cyber event to improve their defenses. But not even the best cyber defense programs guarantee protection against determined adversaries. Nor can redlines safeguard critical infrastructure. Cyber conflict is being waged in the shadows—but the danger is clear enough. Digital cloak-and-dagger operations, fueled by rising geopolitical tensions, threaten to undermine trusted IT systems, connected devices, and operational technology (OT), potentially causing physical effects.

Adversaries view the federal government, intelligence agencies, the military, and all critical infrastructure industries as one large target-rich environment—one cyber battlespace. To gain the advantage, the United States, allies, partners, and the private sector must create unity of effort. This requires urgent progress on three fronts: fostering operational collaboration, focusing innovation, and integrating cyber offense and defense capabilities with other tools of national power to deter and counter threats.

NEITHER NATIONS NOR ORGANIZATIONS CAN AFFORD TO WAIT FOR A CATASTROPHIC CYBER EVENT TO IMPROVE THEIR DEFENSES.

6 DAYS

The duration of the Colonial Pipeline shutdown in the 2021 ransomware incident

Source:
Department of Energy

$10 BILLION

The estimated global economic damage from the 2017 NotPetya cyberattack

Source:
Wired

$193 BILLION

The cost of a global ransomware attack in a severe hypothetical scenario

Source:
Lloyd's

TOP 5 RISK

How cyberattacks on critical infrastructure rank among 2023 global risk perceptions

Source:
World Economic Forum

SIGNS OF PROGRESS— AND KEY OBSTACLES

FOSTERING OPERATIONAL COLLABORATION

PROGRESS

Operational collaboration is about building and leveraging trusted partnerships between government and industry to elevate national cybersecurity through collective action. Stakeholders in government and industry have been striving to achieve this ideal for years. Early information-sharing success stories like responses to threats from **Hidden Cobra and Cozy Bear** have been succeeded by the achievements of CISA's **Joint Cyber Defense Collaborative (JCDC)**, which aims to unify cyber defenders worldwide, and the National Security Agency's (NSA) **Cybersecurity Collaboration Center (CCC)**, which focuses on protecting the defense industrial base and sensitive government systems. When the Log4j vulnerability came to light in 2021, the JCDC enabled rapid sharing of indicators of compromise, threat activity, and intelligence. And in 2022, the CCC nearly tripled its partnerships to harden almost 2 billion endpoints against nation-state threats. Further, CISA has shown resolve by prioritizing operational collaboration in its **strategic plan**.

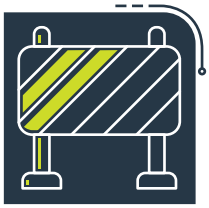
OBSTACLES

Much work remains to be done across the public and private sectors to strengthen ties and build trust. It's been nearly a decade since the Obama administration issued an executive order on cybersecurity information sharing to spur the creation of cross-sector sharing hubs, and since Congress passed the Cybersecurity Information Sharing Act of 2015 with liability protections for industry. But the essence of the challenge has not changed. Critical infrastructure companies are still seeking more timely and actionable cyber threat intelligence and insights from the government, while the government remains concerned that companies are not sharing enough information about the cyber threats targeting private-sector data, networks, and operations. Businesses must trust that sharing information with the government will improve collective cyber defense, not trigger penalties, and the government needs to provide greater assurances to that effect. Achieving operational collaboration will require breaking down barriers across the people, process, and technology dimensions of cybersecurity and questioning longstanding assumptions about information sharing. Agencies should focus on identifying and understanding impediments and defining pathways to overcome them.

FOCUSING INNOVATION WHERE IT'S NEEDED MOST

PROGRESS

Innovation is easy to lionize in principle but hard to tame in practice. The White House has **committed** to increasing investment and expediting technology development in cybersecurity and other industries in the future. Also, the Defense Advanced Research Projects Agency (DARPA) is playing a key role in coordinating the development of innovative cyber capabilities for both offense and defense. The expanded collaboration between DARPA and U.S. Cyber Command (CYBERCOM) in the new **Constellation program** holds great promise. The program is all about accelerating the development of new capabilities through rapid prototyping and integration. In addition, the innovation arms of **DOD**, the Department of Homeland Security (**DHS**), and **CISA** are all partnering with industry to develop cyber solutions.



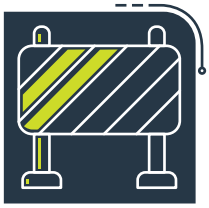
OBSTACLES

For organizations looking to outpace threats, acquiring truly novel solutions is a real challenge. Even the U.S. government's commitment to cybersecurity is no guarantor the latest innovations will be put in place where and when they are needed most. Beset by buzzwords and vendor hype, federal agencies spend billions of dollars chasing shiny objects that seldom produce measurable security improvements for vital missions. The government should make targeted investments in leading cyber capabilities, safeguard the technology, cultivate crucial industrial base elements, and aim to deploy novel solutions that help the government and private sector protect missions and critical infrastructure. Further, stakeholders should apply the concept of innovation more broadly—not only to technology but also to cyber strategies and processes.

INTEGRATING OFFENSE AND DEFENSE

PROGRESS

CYBERCOM marked a key milestone in 2022: With the consent of Ukraine, the Cyber National Mission Force (CNMF) deployed its largest-ever hunt forward team. The team hunted for malicious cyber activity on Ukrainian networks, working alongside Ukrainian cyber experts. The effort enabled disruption of malicious activity before it could cause harm. In addition, insights and adversarial tools and capabilities "were shared with U.S. domestic interagency and public/private industry partners to improve U.S. homeland cyber defenses," **according to the command**. This is a major step in the right direction.



OBSTACLES

Defensive and offensive operational planning functions across federal, intelligence, and defense agencies are too often siloed in terms of missions, resources, and capabilities. This creates uneven cyber defensive readiness where some agencies are less capable and knowledgeable when dealing with advanced adversaries. What's more, this disconnect makes it harder for the owners of offensive cyber missions to benefit from data and insights generated during defensive operations and to leverage best-in-class solutions for their offensive missions.

WHAT'S NEXT:
STEPS TO TAKE NOW

Widespread cyber insecurity is one of the **top global risks** in the near term and for the next decade. Here are steps that leaders can take now to build security, resilience, and cyber superiority:

FOSTERING OPERATIONAL COLLABORATION

- The public and private sectors must focus on achieving tangible outcomes. Although there is a need for some regulation, stakeholders must guard against sacrificing agility and effectiveness on the altar of bureaucracy. To protect the nation's most important critical infrastructure, the majority of which is owned and operated by the private sector, the Biden administration is expected to use its National Cybersecurity Strategy to make the case for expanded regulatory authorities. In doing so, the administration must ensure that emerging regulation does not undermine industry's willingness to participate in cybersecurity information-sharing processes and partnerships.
- The government and the private sector should collaboratively develop an approach that ensures both the public and private sectors gain significant value from sharing threat data and insights. Trust is so difficult to achieve—both sides must give to get this right.
- CISA and the NSA could significantly strengthen progress by rapidly reaching a consensus on a collaborative environment for sharing cyber threat information among government and industry stakeholders. Report language tied to the Fiscal Year 2023 National Defense Authorization Act calls for a study on how best to implement the idea, which originated with the U.S. Cyberspace Solarium Commission. It will not be easy, but this is an opportunity to create unity of effort.

FOCUSING INNOVATION

- DHS should leverage the Homeland Security Advisory Council's **study** on building a more robust "Homeland Security Technology and Innovation Network" to find new opportunities to support the development of novel cybersecurity solutions for critical infrastructure.
- DOD should support national cybersecurity with its forthcoming National Defense Science and Technology (S&T) Strategy. "Cyber" is in the name of just one of **14 critical technology areas of focus**. But many other listed areas—quantum science, future-generation wireless technology, and trusted artificial intelligence, for starters—tie in with national cybersecurity. Opportunities to advance cyber defense and offense with S&T should be top of mind as DOD crafts S&T priorities—and as the Defense Innovation Board performs its related **independent assessment**. DOD should also seek to continue advancing cyber innovations through **strategic investment capital**.
- DARPA and CYBERCOM's **Constellation program** and related efforts to develop leading tools for cyber offense and defense should be well resourced by Congress over the long term. This program is likely to equip the U.S. with essential tools for carrying out the policy of integrated deterrence, a vital element of the National Security Strategy and the National Defense Strategy. Any progress in capability development might also ultimately enable better integration of offensive and defensive operations.
- As discussed at the 2022 **Cyber Beacon** event hosted by the College of Information and Cyberspace (CIC) at National Defense University (NDU), DOD should do more protect the thin sliver of the U.S. industrial base that possesses world-class expertise researching zero-day vulnerabilities. When tapping researchers to reliably

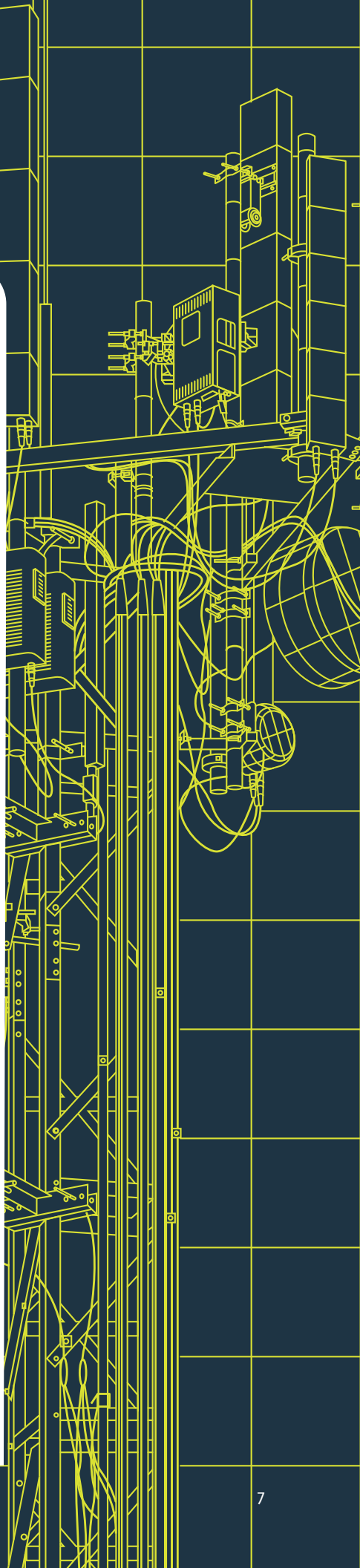
develop zero-days for intelligence and military missions, the U.S. government should prioritize working with U.S. firms. Also, the U.S. should provide more counterintelligence support to these researchers, who are being targeted by foreign spies.

- Agencies and companies should adopt leading strategies such **data-driven cybersecurity** and **zero trust**. For the latter, organizations should start by using a zero trust assessment framework to identify areas where improvement is most needed. Along the way, organizations lagging in cybersecurity fundamentals must be brought up to par.

INTEGRATING OFFENSE AND DEFENSE

- The U.S. should continue the dual-hatted arrangement in which CYBERCOM and NSA are led by the same four-star general. In addition, the nation should leverage this arrangement's inherent speed and agility, as well as the CNMF's recently elevated importance as a **subordinate unified command**, to further advance the integration of offense and defense.
- The nation should plan, fund, and create a dedicated **cyber intelligence center** at CYBERCOM to focus on foreign cyber forces and extremist groups and provide intelligence support to both defensive and offensive cyber operations. Over time, this center could also help attract and grow cyber talent to meet long-term needs.
- Leaders should strengthen the sharing of cyber intelligence and insights across the federal government to better inform U.S. analysts and operators and pursue expanded operational collaboration with critical infrastructure sectors that enables synchronization.
- The government should increasingly leverage national-level cybersecurity exercises and wargames to stress test synchronization efforts, including in crisis response scenarios.
- The U.S. should integrate offensive and defensive cyber capabilities with other tools of national power to deter and counter hostile cyber activities.
- The U.S. should work closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve cyber resilience, and to build collective capabilities to rapidly respond to attacks.

The future of national cybersecurity depends on a unified approach to protect what adversaries see as one cyber battlespace. It depends on operational collaboration, innovation, and the integration of offense and defense. Most importantly, it depends on you and your organization. The steps taken today to build U.S. cyber superiority will make all the difference tomorrow.



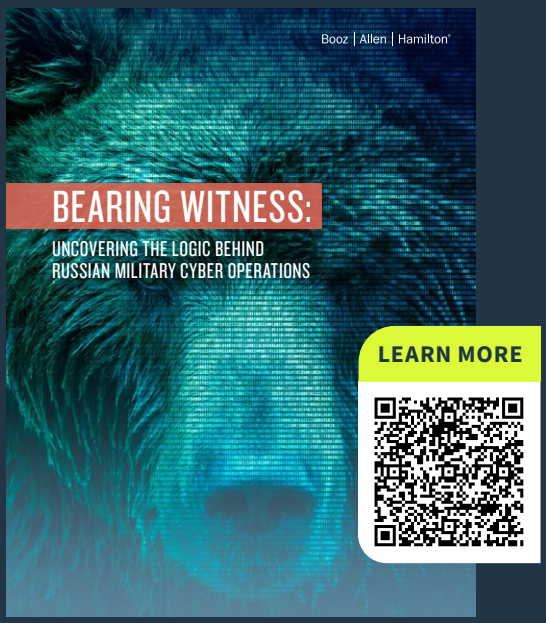
Booz Allen®

INTERESTED IN THE LATEST THREAT INTELLIGENCE?

Download the reports below to discover insights into nation state-sponsored cyber activity, predictions for what's next, and guidance on how to use this historical data to anticipate and plan for future cyber risks.

Same Cloak, More Dagger:
Decoding How the People's Republic of China Uses Cyberattacks

How to prepare today for cyber threats from China



Bearing Witness:
Uncovering the Logic Behind Russian Military Cyber Operations

Insights into Russian cyber activity, predictions for what's next, and guidance on how to use this historical data to anticipate and plan for future cyber risks

HOW TO OUTPACE CYBER THREATS TO CRITICAL INFRASTRUCTURE

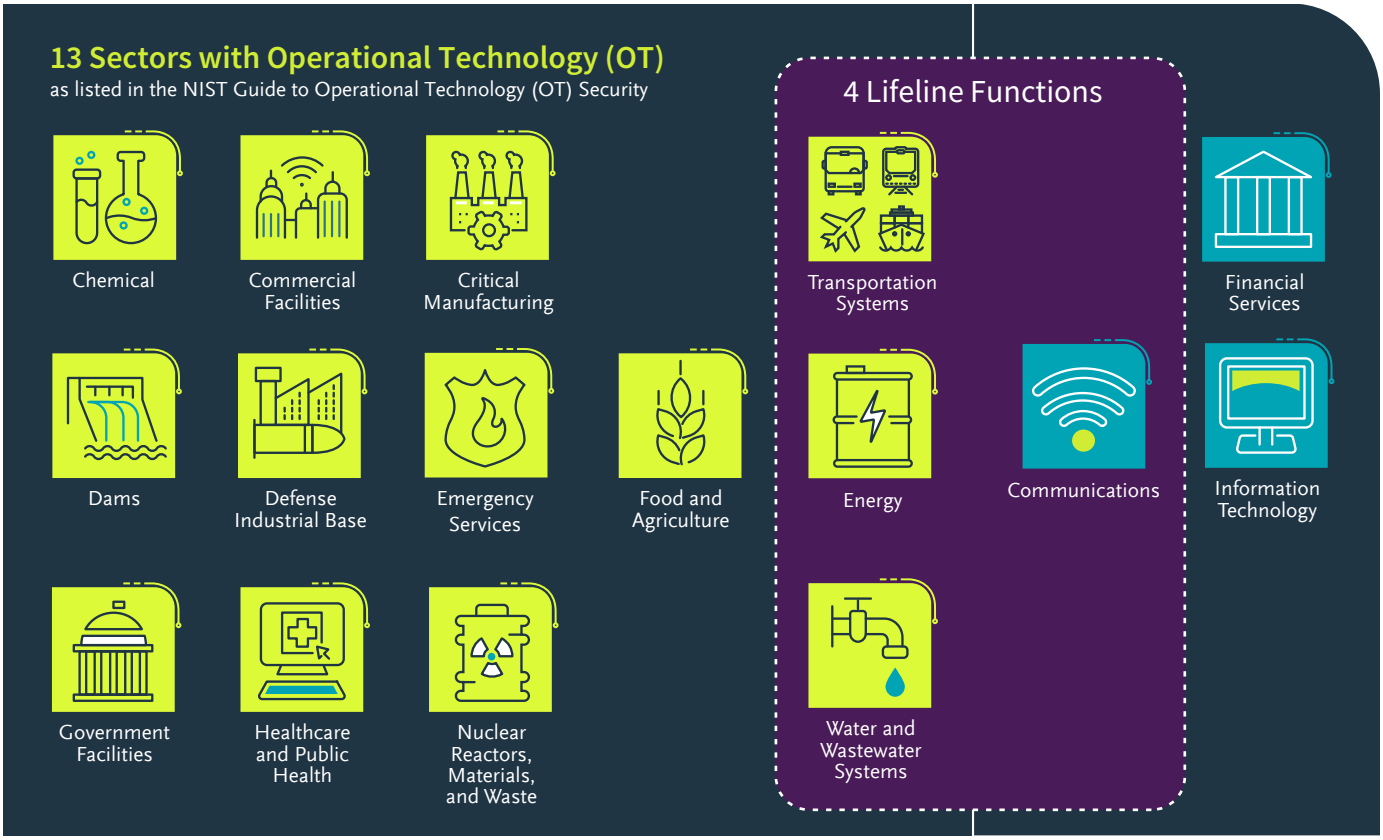
An OT/ICS guide to uncovering and managing systemic risk

Cybersecurity for critical infrastructure has reached a turning point. It's clearer than ever that today's cyber threats drive tomorrow's national security risks. Adversaries surreptitiously target the software, hardware, and services that vital industries rely on. They're seeking ways to sabotage lifeline functions like energy and water to achieve geopolitical and military objectives. The cybersecurity decisions that government and business leaders make today, or put off, could one day be decisive in conflict, crises, or competition. This is why the Joint Cyber Defense Collaborative (JCDC) 2023 Planning Agenda sets specific priorities for reducing systemic risk.

These **priorities** include securing operational technology and industrial control systems (OT/ICS), mainly from open-source software (OSS) risks; advancing cybersecurity and supply chain risk management, particularly for small- and medium-sized businesses; deepening operational collaboration in the energy sector; and protecting edge devices in the water sector. The overall aim is to reduce the spread of risk across interdependent systems so a failure of one area doesn't cause system-wide consequences. For critical infrastructure businesses, however, these priorities are about both risk and reward: They add up to an emerging opportunity to better sustain operations with grace under pressure and advance strategic business objectives.

The world runs on OT/ICS. These systems are largely owned and operated by the private sector. They support day-to-day operations for many control system processes like oil and gas exploration, production, distribution, and refining; electric power generation, transmission, and distribution; and water, wastewater, and public utilities. They're particularly crucial in "lifeline functions"—the four designated sectors where disruption or loss would trigger severe cascading effects on other sectors—but they're also used in many other industries. By strengthening the security and resilience of these systems against emerging cyber risks, businesses can advance national security and their own efforts to thrive and stand out in the marketplace.

THE 16 CRITICAL INFRASTRUCTURE SECTORS



Most business and cyber leaders aren't confident their organization is cyber resilient, according to the World Economic Forum's **research**: Many say their organization needs strong growth and improvement in cyber resilience despite following common practices, while others either have concerns or believe their organization isn't cyber resilient. Also, more than half say the third-party entities they depend on in their supply chain are less cyber resilient than their own organization. Moreover, most of the leaders surveyed doubt their board of directors can uphold a duty of care when it comes to cybersecurity. But now organizations can use JCDC's priorities to inform internal deliberations about emerging cyber risks in the C-suite and the boardroom and foster more confident management of these challenges with security and resilience.

No single report could ever address all facets of the challenges in the JCDC Planning Agenda, and that is not our goal here. Instead, this guide is intended to help critical infrastructure owners and operators accelerate efforts to uncover and manage systemic risk on the path to a more secure and prosperous tomorrow. It aims to complement cyber defense planning by providing context on trends, insights, on leading practices, and actionable advice on building security and resilience. It may also help inform internal discussions with leadership about cybersecurity investment plans. In addition, we've included practical steps that government and industry leaders can take to advance critical infrastructure cybersecurity by harnessing the power of artificial intelligence (AI).

KEY TRENDS

Cyberattacks on critical infrastructure are now top of mind around the world: They rank among the top five risks in the World Economic Forum's 2023 list of global risk perceptions. Also, cyberattacks on the United States rank among Americans' greatest concerns in the 2023 Munich Security Index global survey findings.

In our view, several longstanding trends, and a few newer ones, have shaped the current state of affairs.

Trends in Cybersecurity for Critical Infrastructure

- The IT/OT convergence of cyber and physical systems has outpaced cyber risk management.
- Legacy systems and OSS programs aren't designed to meet today's cybersecurity standards.
- Supply chains—for software and beyond—are vast, growing, opaque, and being subverted.
- Attack surfaces keep expanding: IoT (many kinds), 5G, cloud, OT/ICS, and remote work.
- Organizations are drowning in security data—not maximizing its potential.
- Trust gaps pose persistent obstacles for collaboration.
- Regulation is likely to increase and be consistent with the National Cybersecurity Strategy.
- Determined hackers keep innovating (e.g., tactics, techniques, procedures, and technology).
- Emergent malicious tools are designed to exploit OT/ICS vulnerabilities at scale.

OT/ICS THREATS: A CLOSER LOOK

Common types of ICS include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC). Executives know these systems need protection, but gaining visibility and securing diverse OT/ICS networks is very challenging. Meanwhile, threat actors can easily access devices and designs, exploit vulnerable IT elements, abuse external connections and remote-access capabilities that have expanded attack surfaces, and employ increasingly dangerous hacking tools.

Now, threats are intensifying. The U.S. intelligence community's **latest annual worldwide threat assessment** is "particularly focused on improving its ability to target critical infrastructure," including undersea cables and ICS, and the People's Republic of China (PRC) is "almost certainly ... capable" of launching cyberattacks that could disrupt U.S. critical infrastructure, "including oil and gas pipelines, and rail systems."

Here is a look at how threat actors typically plan and carry out compromises against critical infrastructure control systems based on a five-step framework **articulated** by the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA):

1. The adversary establishes the intended effect and picks a target. These plans will vary by the actor. While nation-states seek geopolitical advantages, ransomware groups recognize that OT networks are among the most valuable assets owned by critical infrastructure businesses, so they target these networks to spark quick ransom payments.
2. The adversary collects intelligence about the target system by conducting open-source research, using insider threats, or hacking enterprise networks. Forget the old cybersecurity adage about "security through obscurity." Hackers might find OT devices using Shodan, Censys, or other obtainable scanners. Metasploit is now integrated into Shodan and contains several OT exploit modules ready for use. Also, hacker forums share videos, tools, and tradecraft so novices can learn attack methods.
3. The adversary prepares to compromise the target by first developing and practicing techniques and tools that can be used to navigate and manipulate the system once initial access is gained. The tools may be readily available or custom built.
4. The adversary gains initial access to the system, often by abusing remote access capabilities designed to give vendors, integrators, service providers, owners, and operators access to the system.
5. The adversary executes techniques and tools to create the intended effect, such as disrupting, disabling, denying, deceiving, and/or destroying the system.

A key concern is the recent discovery of malware designed to exploit OT/ICS vulnerabilities at scale. Traditionally, OT exploits were bespoke and heavily tailored to the target environment (e.g., Stuxnet). But the IT/OT convergence has led developers of discrete products to reuse code and functionality—including OSS—inadvertently creating widespread shared vulnerabilities and risks in the marketplace. In 2022, it was revealed that advanced persistent threat (APT) actors had created a malware toolkit known as Pipedream (or Incontroller) that is capable of endangering countless OT/ICS targets with an array of automated malicious actions.

Pipedream exploits a reliance on common industrial network protocols (including some open-source protocols) in ICS vendor software supply chains. By using standard protocol functions, the toolkit acts like a "legitimate client or a development environment for programming the controller," according to a Codesys security advisory. Once an adversary gains initial access, the tools can be used to scan, compromise, and control targeted OT devices. These tools "have a modular architecture and enable cyber actors to conduct highly automated exploits against targeted devices," the U.S. government **warned**. Given that the malware is based on software widely used in PLCs, it is **reportedly** adaptable to "work in almost any industrial environment." Moreover, Pipedream was **reportedly** part of a Russia-linked operation targeting U.S. electric and gas facilities. Without commenting on reports about the operation, a senior Department of Energy official **said** Pipedream "was, in many ways, a fundamental shift in the cyber capabilities that are out there." The official cited the toolkit's ability to "take advantage of normal processes in systems across the board to potentially cause destructive effects."

There have been other software supply chain risks to OT/ICS security. The widely publicized Log4Shell vulnerability in the Java-based logging package Log4j, which came to light in 2021, affected a wide range of IT and OT systems. Log4Shell isn't primarily known as an OT vulnerability, but it's embedded in countless commercial software products that use open-source code. This shows how OSS ICS vulnerabilities can be tied to broader issues affecting all kinds of systems. Other examples of software-related ICS security challenges include code dependencies revealed in recent years: Urgent11, Ripple20, Amnesia33, and BadAlloc.

Examples of Software Supply Chain Risks Affecting OT/ICS

Urgent11	Ripple20	Amnesia33	BadAlloc	Log4Shell	Pipedream
2019: Major OT vendors relying on real-time operating systems (RTOS) are affected by network protocol vulnerabilities in the Interpeak IPnet TCP/IP* stack. Exploitation could allow remote code execution.	2020: Many ICS devices are affected by vulnerabilities in the Treck TCP/IP* stack. Exploitation may allow remote code execution or exposure of sensitive information.	2020: Many connected devices are affected by vulnerabilities embedded in open-source TCP/IP* stacks. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.	2021: Memory allocation vulnerabilities in multiple RTOS and supporting libraries could be exploited to create unexpected outcomes like a crash or a remote code injection/execution.	2021: An OSS vulnerability affects consumer and enterprise services, websites, applications, and OT products. An unauthenticated remote actor could exploit the vulnerability to take control of an affected system.	2022: An APT malware toolkit exhibits the capability to gain full system access to multiple ICS/supervisory control and data acquisition (SCADA) devices by exploiting common protocols, including open-source protocols.

* *Transmission Control Protocol/Internet Protocol*

Source: CISA advisories

Ultimately, no one organization or sector can manage such risks alone. For instance, industries such as electricity and natural gas need to increase cross-sector coordination on supply chain risk management related to commonly used hardware and software inputs, according to the National Infrastructure Advisory Council of industry and government executives. More cross-sector analysis is needed to better understand how simultaneous equipment failures across multiple modes or sectors sparked by a common cause could trigger unanticipated widespread consequences, the panel concludes in a **recent study**.

UNCOVERING AND MANAGING SYSTEMIC RISK

So how can critical infrastructure organizations uncover and manage systemic risk issues captured in JCDC's Planning Agenda? The following table lists ideas for consideration. It is important to note that different organizations will have varying risk management maturity levels in different areas. When in doubt, performing an initial assessment can help an organization gauge maturity in a particular area, and plan targeted improvements.

Challenge	Uncover	Manage
Detect and address today's ICS threats	Traditional cyber protection mechanisms aren't always feasible for ICS. Gaining visibility into these environments to support cybersecurity is critical. But few OT environments have any advanced cybersecurity monitoring in place. It's essential to understand the **common challenges** in ICS threat detection: • Legacy equipment and vendor restriction limit endpoint tool coverage. • Sensitivity in ICS environments requires many tools to be passive. • No one tool/sensor can provide visibility into all threats. • Limited cybersecurity skills in operations and plant operations knowledge in the security operations center (SOC). • Threats are constantly changing, and adversaries are advancing techniques. OT monitoring requires a holistic solution. **Guidance** from the NSA and CISA can help organizations understand tactics, techniques, and procedures (TTP) that threat actors use to compromise **OT/ICS** assets, as well as recommended mitigations.	Identifying which parts of the organization have critical data and assets and prioritizing their security is essential. Build a robust capability that enables threat detection within the ICS environment using a combination of passive and active monitoring tools. Also, build out playbooks, processes and training needed to enable collaborative response efforts. Conduct regular ICS-focused tabletop exercises to practice these playbooks and hone skills. A four-step approach to building an ICS threat detection and response program involves creating a strategy, expanding visibility in the networks (including gaining an understanding of what normal looks like in your environment), enabling continuous detection and response functions, and facilitating effective response operations. A well-thought-out strategy contains an initial list of targeted use cases, a rollout plan containing a proof-of-concept phase, skill sets needed to perform the work, staff required to enable the work, and a basic timeline. Leverage CISA's **Guide to Securing Remote Access Software**, as well as lessons from the **Cyber Storm national exercise**. Also, select entities may be eligible for **CyberSentry**, a voluntary CISA-managed threat detection and monitoring capability for critical infrastructure IT/OT networks.
Explore opportunities to adopt zero trust	If an attacker can reach an OT/ICS system, the defender has in a sense already lost, which underscores the importance of network segmentation, isolation, threat detection, and **a zero trust cybersecurity mindset**. Embracing zero trust is about stepping up and owning the risk that threats can emerge inside, not just outside, traditional network boundaries—and it's about proactively countering these risks. There are three principles of zero trust: assume a breach; never trust, always verify; and allow only least-privileged access based on contextual factors. Cybersecurity teams can't just buy a zero trust architecture (ZTA) from a vendor. Instead, teams must scrutinize an organization's strengths and challenges with intention, and then chart a path to a ZTA while committing to a longer journey.	The **seven zero trust pillars** are aligned with the Department of Defense (DOD) zero trust **reference architecture** and CISA's **maturity model**: • User • Device • Applications and Workloads • Network/Environment • Data • Visibility and Analytics • Automation and Orchestration Using the pillars and governance combined with a zero trust maturity assessment model, you can rate the maturity of current capabilities in all seven zero trust dimensions. Applying zero trust to OT environments is an area of increasing interest, as this **recent article** from Idaho National Laboratory shows.

Challenge	Uncover	Manage
Improve supply chain risk management	Know your supply chain. Establish and maintain full awareness of the suppliers—including third, fourth, and fifth parties—who participate in the design, development, implementation, maintenance, and disposal of all products and services. Also, explore using the **MITRE System of Trust Framework**, which seeks to define, align, and address the specific concerns and risks that prevent organizations from trusting suppliers, supplies, and service providers. Manufacturers and suppliers of software used by critical infrastructure IT and OT/ICS should consider producing a software bill of materials (SBOM).	Apply new supply chain knowledge to inform more effective risk management. Prioritize risks. Conduct multifaceted, ongoing monitoring. Drive remediations quickly. Integrate these efforts into enterprise risk management. Leverage **guidance** from CISA. Apply the **SBOM** concept to reduce software supply chain risks. SBOMs will be crucial for providing organizations with the greater visibility they seek and enabling threat hunting. Also, support the spread of cybersecurity supply chain risk management (**C- SCRM**) practices via the related NIST National Cybersecurity Center of Excellence (NCCoE) **project**.
Proactively counter software supply chain threats	Consider using the **Trident Framework**, which depicts the sort of cross-functional effort needed to counter software supply chain threats. It shows how enterprises can build a unified defensive effort involving cybersecurity experts, acquisition professionals, and the chief information security officer. The first step for an organization aiming to create this digital trident is to implement an SBOM framework that meets the National Telecommunications and Information Administration's minimum elements.	Apply the **framework's five-step process** to proactively hunt for software supply chain threats. Along the way, threat hunters should glean lessons from use cases. Also, they should study, contribute to, and build data sets around software supply chain attacks. **Put lessons and insights into action** by developing informed hypotheses to start the hunt.
Double down on cybersecurity fundamentals	The need to uncover cyber risks by strengthening cybersecurity fundamentals cannot be understated. A 2022 **assessment** based on a survey of 1,200 executives from a range of industries found that only a third of organizations were implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework at an advanced level (and only 4 in 10 organizations had built their cybersecurity program on zero trust principles). Moreover, the Government Accountability Office **reported** last year that only three of 16 sector risk management agencies had determined the extent of their sector's adoption of the NIST Framework. Review **CISA Risk and Vulnerability Assessments (RVA)** to learn more about common attack methods and security gaps.	Look for opportunities to use the **NIST Cybersecurity Framework** to its full potential while also adopting **CISA's cross-sector voluntary Cybersecurity Performance Goals (CPGs)**. These goals are grouped using the five functions of the NIST framework. Examples of goals include changing default passwords; implementing phishing-resistant multifactor authentication (MFA); separating user and privileged accounts; and creating, maintaining, and exercising cybersecurity incident response plans. You can also learn more about **ongoing efforts** to update the NIST Framework and provide input where appropriate. In addition, small- and medium-sized businesses can leverage **CISA** and **NIST** guidance.
Adopt data-driven cybersecurity	Today, many security teams can't make the most of their data and hence can't deliver value for the entire organization. Teams are forced to choose which data to collect when technology advancements and security budgets are out of sync. And that means **agencies** and critical infrastructure **entities** are losing ground to worsening digital threats—because they aren't using data as an asset.	Begin to unlock the potential of your security data, recognizing the potential to advance strategic objectives. Businesses that embrace data-driven cybersecurity can gain a competitive advantage. Conduct an analysis and make the data available to whoever needs to consume it. Data access should be controlled centrally. Start normalizing data to provide better visibility into the enterprise.

Challenge	Uncover	Manage
Boost security and resilience for edge devices	In the water sector, for example, improve asset management by ensuring: • The OT equipment and software inventory includes offsite and remote devices • The asset management plan includes devices and equipment from external vendors • PLCs and sensors receive security updates as needed • Automatic update installation is functioning where feasible • Inactive devices are removed from the network • The entire operational configuration is backed-up or archived	Leverage cybersecurity capabilities such as firewalls with intrusion detection, edge security, and virtual private networks. Follow the (NCCoE) **project** on how the water sector's adoption of automation, sensors, data collection, network devices, and analytic software may also expand cyber vulnerabilities and related risks: Watch for recommendations on asset management, data integrity, remote access, and network segmentation. For 5G-specific questions, see content on **establishing a secure and resilient ecosystem**, **enabling continuous monitoring**, and **zero trust**.
Apply AI to spot and address vulnerabilities	Both government and industry can find new opportunities to apply AI to critical infrastructure cybersecurity by revisiting the concepts associated with the Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge, which aimed to build automatic defenses. For instance, to improve vulnerability identification and characterization, the government should consider investing in AI systems designed to accurately predict the likelihood that a vulnerability will be exploited. Also, current DARPA efforts to identify, characterize, model, and measure exploitable vulnerabilities in widely used mobile devices could be a good template for future government efforts to address critical infrastructure cybersecurity gaps.	To support the development of effective defensive cyber and monitoring solutions, the nation should foster greater connections between the data science and AI community and stakeholders across the nation's critical infrastructure industries. This would raise awareness about key nuances inherent in attacks on specific sectors, enabling developers to create tailored solutions to meet specific mission needs. Also, organizations should aim to use AI to augment (rather than replace) existing cyber tooling. And to strengthen remediation, the government and industry could consider large-scale investments that build on DARPA Grand Challenge findings about options for including more computer autonomy in cyber defense. DARPA's recently announced **AI Cyber Challenge (AIxCC)** is a step in the right direction.
Anticipate future threats	Proactively research the threat landscape as it applies to your industry, organization, and environment. Close knowledge gaps about technology, vulnerabilities, and malicious activity with open-source intelligence, including reports tailored to meet your organization's needs. Track alerts from **CISA**, other authorities, and cyber information sharing and analysis centers (ISACs). Review insights on **China's cyberattack strategy** and the logic behind **Russian military cyber operations**.	Adopt an intelligence-driven, threat-informed approach to cyber risk management, including exercises with realistic red teaming that leverage catalogs of the latest known vulnerabilities affecting networks, hardware, and software. Organizations lacking access to a sophisticated red team may benefit from using micro emulation plans developed for defenders by **MITRE Engenuity**.
Expand operational collaboration	Set the stage to collaborate. The more you know about the threat landscape and vulnerabilities as they apply to your organization through proactive research and beyond, the better positioned you are for greater operational collaboration within a given industry and across sector boundaries.	Commit to building trust and sharing actionable intelligence and insights on cyber threats. Craft the architectures that will facilitate and simplify collaboration: Beyond culture changes, technical architectures are key because if they're not in place, their absence becomes an obstacle to collaboration. In addition, leverage recent **National Infrastructure Advisory Council (NIAC)** recommendations for boosting cross-sector collaboration.

NEXT STEPS

Here are steps leaders can take now to help critical infrastructure organizations outpace cyber threats:

1. To advance ICS threat detection and response, create a high-level strategy before any people, process, or technology changes occur. A well-thought-out strategy contains an initial list of targeted use cases, a rollout plan containing a proof-of-concept phase, skill sets needed to perform the work, staff required to enable the work, and a basic timeline. Expand/maintain visibility into the environment. Baseline what "normal" looks like. Establish response rules of engagement and define what actions can be taken/escalated. Consider prepositioning incident response tools to expedite response and recovery.
2. Assess your organization's zero trust maturity. Also, watch for future federal guidance on applying zero trust in OT environments.
3. Assess your supply chain to truly understand it and its component parts, several layers down. Also, support emerging efforts to better understand and manage supply chain risk across sector boundaries.
4. Prioritize threat hunting for software supply chain threats.
5. Maximize the potential of the NIST Framework and CISA CPGs.
6. Assess opportunities to adopt a data-driven cybersecurity approach.
7. Leverage NCCoE insights to boost the security and resilience of edge devices.
8. Government leaders should consider funding and launching new initiatives that advance AI cybersecurity capabilities for critical infrastructure by building on the successes of past and current DARPA initiatives. Industry should prioritize participating in such initiatives while also making complementary investments.
9. Assess whether your organization fully leverages open-source intelligence (OSINT) research, collaboration, and anonymized cybersecurity data sharing to inform cyber risk management. Participate in sector-based information sharing and analysis centers (ISACs) to exchange data, insights, and leading practices about threats and mitigation strategies. Also, pursue opportunities to collaborate across sector boundaries.
10. Support better performance-based pressure testing in critical infrastructure sectors such as water and energy to help these sectors make needed investments in cybersecurity rather than postponing investments for fear of passing on costs to consumers. Conduct regular tabletop exercises to evaluate operational readiness and inform cybersecurity budget plans and decisions. Also, support the development of cross-sector cybersecurity drills.

Booz Allen®

THE NATION IS AT RISK.

SECURITY STARTS WITH CYBER.

Every day, Booz Allen uses mission understanding, battle-tested approaches, and ready-to-deploy solutions to disrupt the way our country tackles cybersecurity. We are constantly evolving alongside the adversary. We pay close attention to their techniques, technologies, and tactics to help you stay ahead of threats, harden your critical systems, and defend what matters most.

See our approach at **BoozAllen.com/NationalCyber**

LEARN MORE

PUTTING ZERO TRUST INTO PRACTICE

Fitting the pieces together for advanced cyber defense

Federal agencies are racing to adopt a zero trust architecture to comply with urgent cybersecurity requirements. Some are further along than others in this journey, but all face the same questions: Where do we start? And how do we move our organization to the necessary architecture?

To answer these questions and pinpoint where improvements are needed, organizations must first step back and review their existing cybersecurity posture and technology roadmaps through a zero trust maturity assessment. This in-depth look at organizational and architectural issues—which provides deeper insights than typical cyber risk reviews—is designed to help organizations identify and address their zero trust gaps.

UNDERSTANDING THE PILLARS OF ZERO TRUST

Identifying zero trust gaps as early as possible will help organizations meet upcoming deadlines. Based on Executive Order 14028 and the federal zero trust strategy, agencies must achieve specific zero trust security objectives by the end of fiscal year 2024. To that end, they have been drafting implementation plans, which need to be refined and resourced to accomplish "ambitious, achievable goals," according to the White House's FY24 cybersecurity budget guidance.

Evaluating the current state of the enterprise's capabilities and gaps is the first step. This enables the security team to weigh priorities and craft tailored implementation guidance to achieve focused improvements over time.

This evaluation requires a framework—a basis for rating capabilities, setting targets for improvement, and achieving measurable progress. To that end, Booz Allen developed a maturity assessment model: It aligns to the Department of Defense (DOD) and Cybersecurity and Infrastructure Security Agency (CISA) maturity models, but provides a more granular look at an organization's capabilities across the seven pillars defined in the DOD reference architecture. For more detail on the pillars, see Figure 1 for a visual summary and examples of capabilities along the spectrum.

The model helps put the principles of zero trust—assume a breach; never trust, always verify; and allow only least-privileged access based on contextual factors—into action. It lets organizations rate their capabilities in all seven dimensions of zero trust using the five maturity levels: initial, minimal, basic, innovative, or leading. Insights from such an assessment can help an agency work toward deploying comprehensive security monitoring, granular dynamic and risk-based access controls, and system security automation in a coordinated way throughout infrastructure.

Armed with a threat-centric understanding of where an organization is along the spectrum, it's possible to set future targets that help drive down operational risk and give rise to new solutions for pressing needs.

Over time, organizations can continuously use the maturity assessment model to conduct follow-on assessments whenever they need to refresh their approach. The first step is always to diagnose challenges across the seven pillars by examining how people, process, and technologies form the organization's security solution. Next, organizations design a zero trust strategy, develop new fixes in the safety of a lab, and deploy new solutions.

The overarching strategy spans the zero trust pillars, provides a unified target state and a multiyear roadmap, and prioritizes the development of strong governance policies that drive enforcement of conditional access.

Elevate Security by Design with 7 Pillars of Zero Trust

Maturity model enables focused improvement, in several steps, from initial practices toward leading capabilities

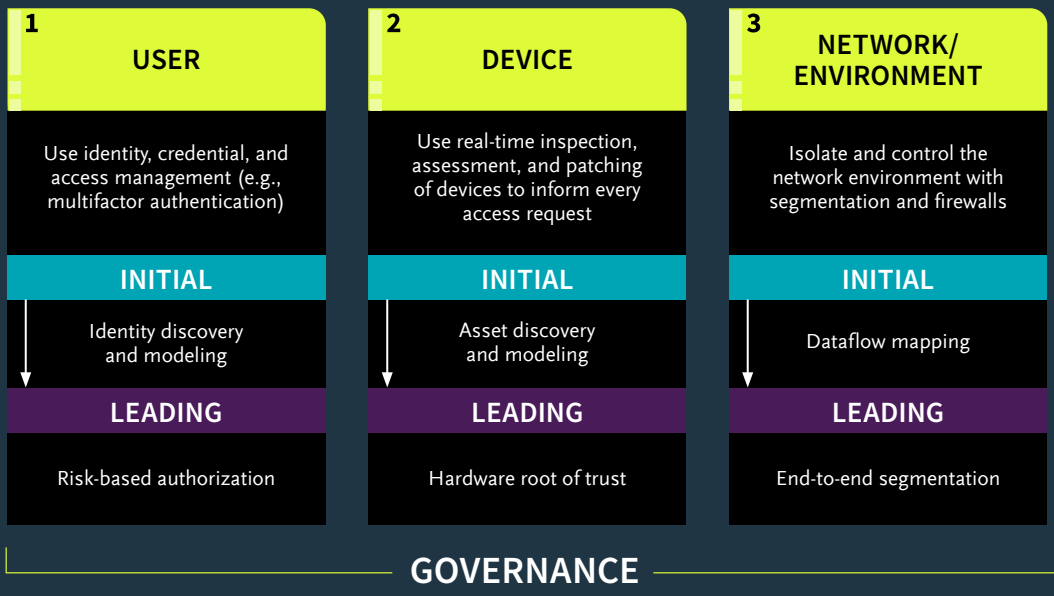


Figure 1

EVALUATING THE CURRENT STATE OF THE ENTERPRISE'S CAPABILITIES AND GAPS IS THE FIRST STEP. THIS ENABLES THE SECURITY TEAM TO WEIGH PRIORITIES AND CRAFT TAILORED IMPLEMENTATION GUIDANCE TO ACHIEVE FOCUSED IMPROVEMENTS OVER TIME.

Booz Allen uses this same approach internally to improve our own security posture. The firm is committed to making Booz Allen "client zero" for the development of all kinds of innovative new solutions as we operate and defend a global enterprise with more than 30,000 users supporting a wide range of critical missions.

TECHNICAL CHALLENGES TO FOCUS ON

Operationalizing a zero trust architecture along the path to maturity brings a host of technical decisions. Amid the multitude of potential priorities, here are three notable areas of focus for cyber and data practitioners.

DEALING WITH DATA

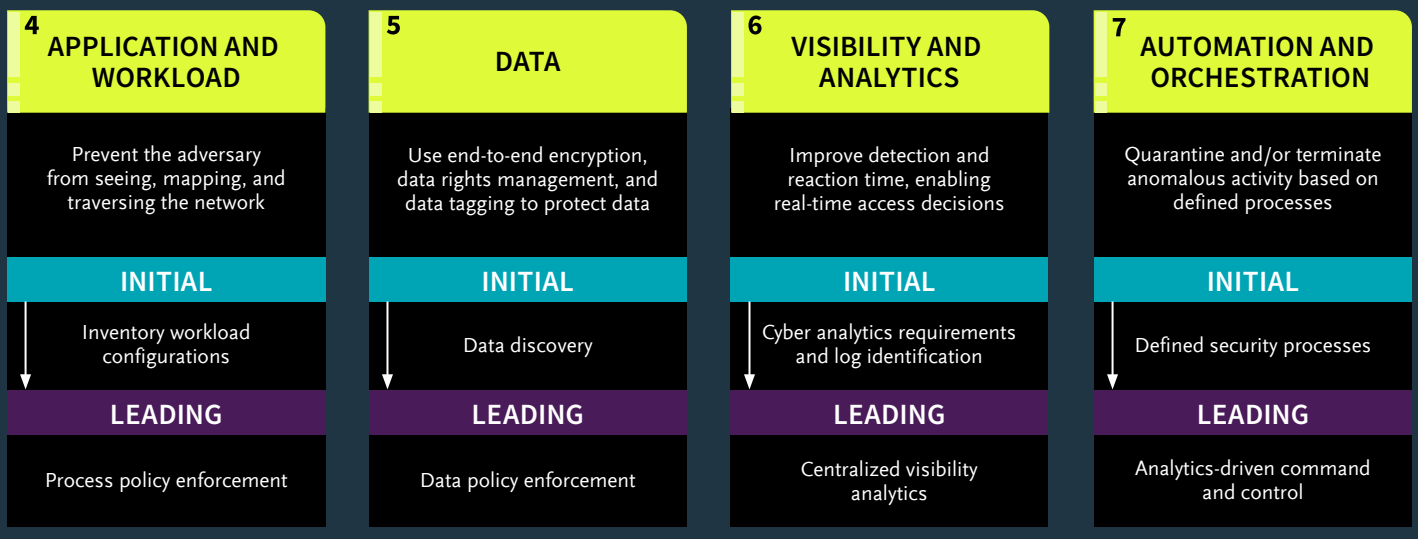
Every organization is unique. But the aspect of zero trust where most organizations tend to be the weakest is the data pillar. This area involves using end-to-end encryption, data rights management, and data tagging to protect data. Organizations should prioritize fixes in the area of data management to ensure the success of broader objectives.

For instance, as organizations try to conduct data discovery and classification, the first area they are looking to modernize is secure access to their networks (cloud and on-premises), otherwise known as zero trust network access (ZTN). To enable restricted access by default as desired, they first need to figure out how to classify and handle their data.

IMPLEMENTING IDENTITY

Another big hurdle for enterprise cybersecurity is implementing identity in an unfamiliar way. To achieve the federal vision for zero trust, agency staff need to use enterprise-managed identities to access the applications they use for work. However, employees change roles, routinely in some organizations. It is important, yet challenging, for security teams to maintain awareness of what these individuals should and should not be able to access based on their new position.

The identity management piece is a vital enabler for all zero trust principles. Strong authentication is also important to provide assurance around identities. Focusing on these areas from the start can set a strong foundation for further zero trust improvements. Also, organizations should establish a single source of truth for



identity credential and access management (ICAM)—one tool that systems can rely on to verify that particular people should have access to particular functions or features. In some cases, based on the size of the organization, federated ICAM solutions are needed.

MAKING THE MOST OF LOGS

Another major challenge is the proliferation of logs driven by zero trust's strong emphasis on continuous monitoring. Amassing countless new logs could overwhelm relatively small security teams. Organizations need to be smart and efficient in how they handle all that data.

Although the administration has introduced new advanced logging requirements, agencies aren't yet using all that data effectively within their security operations centers. On a continuous basis, it's important to evaluate what data is useful and what isn't—for instance, focusing on relevant data elements within broader data feeds.

What's more, organizations need to move away from retaining data in ways that are less cost effective for the long term. By adopting a data-driven cybersecurity approach, organizations can start using cloud-based solutions to store massive quantities of cybersecurity data for longer periods in a more cost-effective manner, which unlocks the benefits of security analytics at scale in real time. And this, in turn, can enable advanced cybersecurity that uses predictive analytics and turns threat intelligence into actionable insights.

Making investments in advanced technology like artificial intelligence (AI), machine learning (ML), and streaming analytics can help security teams make the most of their data, identify aberrant trends in network traffic, and get ahead of threats. For now, federal and defense agencies are just starting their efforts on this front, but increasingly they will be looking to the private sector to leverage such capabilities.

Over time, organizations can work toward implementing the architecture for a cloud-native, cyber-focused data pipeline for streaming analytics (threat hunt, detection, and compliance) and start to apply the principles of zero trust and data-driven cybersecurity to protect 5G and cloud-based networks.

ZERO TRUST IN 5G AND BEYOND

Imagine an adversary is out to steal and sabotage sensitive technology that underpins a major defense acquisition program designed to meet urgent military requirements. It could all start with a threat actor using 5G threat vectors to conduct espionage, compromise the supply chain, infiltrate a network, and move toward the target. Applying a zero trust mindset, however, could counter such threats with stringent authentication measures, network segmentation, and evolved threat hunting. This is one of two hypothetical scenarios our team developed using tactics and techniques from the MITRE ATT&CK® knowledge base to show the potential of **zero trust in 5G**.

Operators of 5G ecosystems need holistic security that includes zero trust architecture, 5G development, security and operations (DevSecOps), and a 5G workforce, as well as vulnerability research and embedded security. Zero trust principles can spread through the entire 5G architecture when analytics and automation are used to drive security improvements over time with policy updates aligned to the other pillars. The continuous development and deployment of new policies protects application authentication and access into the 5G network.

NEXT STEPS

EMBRACE ZERO TRUST WITH CONFIDENCE

The journey to zero trust starts with evaluating an organization's cybersecurity against a maturity assessment model and then designing, developing, and deploying solutions that are fit for purpose. Along the path to maturity, organizations may find certain zero trust capabilities already in place and can leverage near-term opportunities to make headway without significant investment. For more substantial zero trust efforts, there is the ability to request funding via the Technology Modernization Fund (TMF).

Importantly, security leaders can look to zero trust efforts at other agencies to glean lessons learned. For instance, the Defense Information Systems Agency (DISA) is developing a scalable prototype of a zero trust security solution known as Thunderdome. Also, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute for Standards and Technology (NIST) have recently published several pieces of zero trust guidance. As organizations leverage the growing body of federal guidance on zero trust and share lessons learned, U.S. national and economic security is sure to benefit.

- Agencies are drafting zero trust implementation plans to meet specific zero trust security mandates by the end of fiscal year 2024.
- The path to developing tailored solutions for zero trust starts with evaluating the current state of the enterprise's capabilities and gaps. Armed with a threat-centric understanding of where an organization is along the spectrum, it's possible to set future targets that help drive down operational risk and give rise to new solutions for pressing needs.
- Three notable areas of focus for cyber and data practitioners are dealing with data, identity management, and smart, efficient handling of logs and data.

Booz Allen®

WE'RE INVENTING TOMORROW'S NATIONAL CYBER SOLUTIONS—TODAY

At Booz Allen DarkLabs℠, the hardest national cybersecurity problems drive our innovative research and development agenda. Our venture capital-style research and prototyping unit rapidly designs, creates, and tests novel services and solutions—directly aligned to current and emerging cybersecurity needs in national mission areas. We apply our unique adversarial mindset—and insights about the tradecraft used by the world's most advanced hackers—to power innovation as a trusted partner with exquisite national cyber talent.

LEARN MORE

THE FUTURE FIGHT: CYBER ENABLING DECISION ADVANTAGE

How joint and combined cyber forces can achieve greater agility, speed, scale, and effectiveness

The speed and complexity of U.S. full-spectrum cyber operations have grown exponentially since 2016 when it took months to coordinate Operation Glowing Symphony—U.S. Cyber Command's first large-scale cyberattack to take down the global networks of ISIS. This initial use of CYBERCOM's authorities, capabilities, and processes for offensive cyber operations set the stage for today's persistent engagement with adversaries. But deterring or winning future conflicts requires greater agility, speed, and scale, as well as integration of full-spectrum cyber capabilities with other elements of national power and with joint and combined capabilities.

The decisive advantage in future conflict will go to the side that can sense, understand, decide, act, and assess faster and more effectively than adversaries. This is a clear lesson learned from multiple cyber and non-cyber operations conducted since 2001 and reinforced most recently during the Russia-Ukraine War.

U.S. and partner forces must synchronize and integrate kinetic and non-kinetic capabilities at all levels to generate concurrent effects across all domains faster and more effectively than the enemy. This is what the U.S. Army calls "convergence," and achieving it will be a critical differentiator for US and allied forces in future conflict. It will enable the joint force to maintain information and decision advantage; preserve command, control, and communications systems; and ensure critical detection and targeting operations. Full-spectrum cyber forces will play a vital role in achieving convergence.

In any future competition, crisis, or conflict, the importance of the joint/combined force's ability to integrate and synchronize special operations forces (SOF), space, and cyber capabilities across all warfighting domains cannot be overstated. More specifically, DOD's ability to deliver the effects of the SOF-Space-Cyber triad in permissive to denied environments will become critical for national efforts to project power, compete, and deter adversaries while remaining under the threshold of armed conflict.

The 2023 DOD Cyber Strategy describes how the department envisions wielding the nation's military cyberspace capabilities. Since 2018, DOD cyberspace forces, in conjunction with interagency, foreign, and commercial partners, have executed a strategy of persistent engagement; full-spectrum cyberspace operations defending forward, actively disrupting malicious cyber activity before it can affect the U.S. homeland; and, as required, attacking adversaries in and through cyberspace.

To outpace adversaries in all domains the joint/combined force must be able to see itself, see the adversary, and see all other relevant actors, actions, and activities in the operations and information environments—and then act—all at mission-relevant speed and scale. The ability of DOD to deliver the operational capabilities mandated in the DOD Cyber Strategy depends on building a robust full-spectrum capable force enabled by secure and resilient networks, valid data, unique cyber weapons systems and infrastructure, realistic training, and effectively integrating cyber with all other warfighting domains.

National security increasingly depends on effective full-spectrum cyber operations. Cyber forces need to uphold national defense, disrupt and dismantle emerging threats, and collaborate with international partners. DOD and the industrial base have an unprecedented opportunity to build a truly integrated weapons platform that is agile, scalable, interoperable, and resilient. Resalistic training and operations with mission partners will ensure cyber forces can effectively apply their talent and technological capabilities to enable decision advantage. Meeting these needs today will position the joint force to meet the operational needs of the nation.

The **new DOD Cyber Strategy specifies** that DOD's Cyberspace Forces, in concert with partners, must:

- **Defend the Nation.** The Department will campaign in and through cyberspace to generate insights about malicious cyber actors, as well as defend forward to disrupt and degrade these actors' capabilities and supporting ecosystems. Additionally, DOD will work with its interagency partners to leverage all available authorities to enable the cyber resilience of U.S. critical infrastructure and to counter threats to military readiness.
- **Prepare to Fight and Win the Nation's Wars.** The Department will ensure the cybersecurity of the DOD Information Network and will further invest in the Joint Force's cyber resilience. Additionally, the Department will use cyberspace operations to generate asymmetric advantages in support of the Joint Force's plans and operations.
- **Protect the Cyber Domain with Allies and Partners.** The Department will assist U.S. Allies and partners in building their cyber capacity and capability, as well as expand avenues of potential cyber cooperation. DOD will continue to conduct hunt forward operations to build cyber resiliency and will reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms.
- **Build Enduring Advantages in Cyberspace.** The Department will optimize the organizing, training, and equipping of the Cyber Operations Forces and Service-retained cyber forces. Furthermore, DOD will invest in the enablers of cyberspace operations, including intelligence, science and technology, cybersecurity, and culture.

Fact Sheet: 2023 DOD Cyber Strategy

THE FUTURE OF WARFIGHTING: SOF-CYBER TRAINING

Accelerating effective SOF–cyber integration

In any future competition, crisis, or conflict, the importance of the joint force's ability to integrate and synchronize special operations forces (SOF), space, and cyber capabilities across all warfighting domains cannot be overstated. More specifically, SOF's ability to deliver the effects of the SOF-Space-Cyber triad in permissive to denied environments will become critical for national efforts to project power, compete, and deter adversaries while remaining under the threshold of armed conflict. Now more than ever, the readiness of the U.S. military to meet these new operational requirements will depend on the training that SOF cyber operators receive to maximize the triad's potential.

The Department of Defense (DOD) and U.S. Special Operations Command (SOCOM) have begun developing tomorrow's SOF cyber training. In a 2019 memo concerning the governance of cyberspace operational forces, the secretary of defense designated SOCOM's force-generation responsibilities as separate from U.S. Cyber Command's (CYBERCOM) responsibilities for the Cyber Operations Forces (COF) and the Cyber Mission Force (CMF).1 SOCOM has service-like training responsibilities under Title 10 as a joint force trainer and as such must ensure SOF cyber forces are trained, certified, integrated, and interoperable with conventional and other joint forces. SOCOM has made some progress in establishing training requirements, resources, and interoperability standards for the SOF service components and theater special operations commands (TSOCs).

The unique nature of SOF-peculiar cyber operations compared to conventional cyber missions requires the development of skills and capabilities that are not the focus of CMF/COF training, and programs like the Persistent Cyber Training Environment (PCTE) are not architected to meet the needs of SOF cyber. For example, the preponderance of cyber training and exercises across the joint force focus on the tasks of a remote operator leveraging substantial infrastructures to gain access to the target and massive reachback support capabilities to achieve effects. The implementation of SOF-peculiar cyber will occur at or near the target with close physical access being the initial vector and limited-to-no reachback support available. These skills will need to be honed with realistic training that reflects how SOF personnel continuously deploy around the world, in all environments from permissive to hostile, because it is there, at the tactical edge, that SOF cyber operations will occur. SOF cyber is reliant upon other SOF skills to be effective, and the effects of SOF cyber will be more immediate and localized than traditional cyber, thus a unique training and exercise capability that blends the cyber and physical realms, like the SOF Cyber Physical Testbeds capability, needs to be expanded and normalized throughout the SOF training enterprise.

SOF personnel already meet substantial training-and-education requirements to become proficient. SOF operations in the cyber domain will levy additional, substantial knowledge-and-skills requirements. This burden and the likely absence of reachback support create an obvious need to lower the cognitive load on operators and increase lethality via artificial intelligence and machine learning (AI/ML) integration. Thus, SOF cyber training and exercise capabilities will need to incorporate the use of edge-hosted AI/ML capabilities. SOCOM's J3 Joint Collective Training Division (JCT) has begun this effort by incorporating the Booz Allen-developed SOF Operator AI Toolkit into some of their events.

AN INTEGRATED APPROACH TO TRAINING AND EMPLOYING NEW TECHNOLOGIES

SOF cyber forces will play a leading and outsized role in future operations by providing offensive, defensive, and influence capabilities across the full range of SOF missions. As the former SOCOM commander, **Gen. Richard Clarke, stated**, "We need coders ... the most important person on the mission is no longer the operator kicking down the door, but the cyber operator who the team has to actually get to the environment so he or she can work their cyber tools into the fight." While not every SOF operator will become a coder or deliver cyber effects, there is an opportunity to build cyber skills for select personnel while also evolving training for all SOF forces. We have seen the SOF components have already looked internally at how to best develop their ranks to integrate cyber into their core activities. This is a key step toward equipping traditional SOF forces with greater insights about cyber capabilities and what their organic cyber operator teammates need to put these new capabilities into action.

Elite U.S. forces understand the value of realistic training: Accelerating the integration of SOF and cyber in training is a natural next step. By integrating cyber terrain into training areas, SOF teams can gain hands-on experience working with SOF cyber operators to fully understand how to best incorporate new cyber tactics, techniques, and procedures (TTP) into their operations across all SOF missions. SOF-cyber integration should span all SOF core activities, not just direct action and special reconnaissance, but also information operations and irregular warfare. To improve confidence in the value proposition of such integration, cyber activities should not be "white carded"—merely simulated—during training and exercise events: Instead, they should be realistically embedded in live, virtual, and constructive parts of the joint operational and readiness training cycle. Success and failure in realistic environments will accelerate innovation, refine use cases, advance joint interoperability, and increase trust in cyber capabilities.

NEXT STEPS

It takes years to train operational SOF units to the level of proficiency needed to accomplish their missions. Integrating new cyberspace capabilities into SOCOM's forces requires investments in time, resources, and partnerships. To accelerate this integration, the following three recommendations are offered.

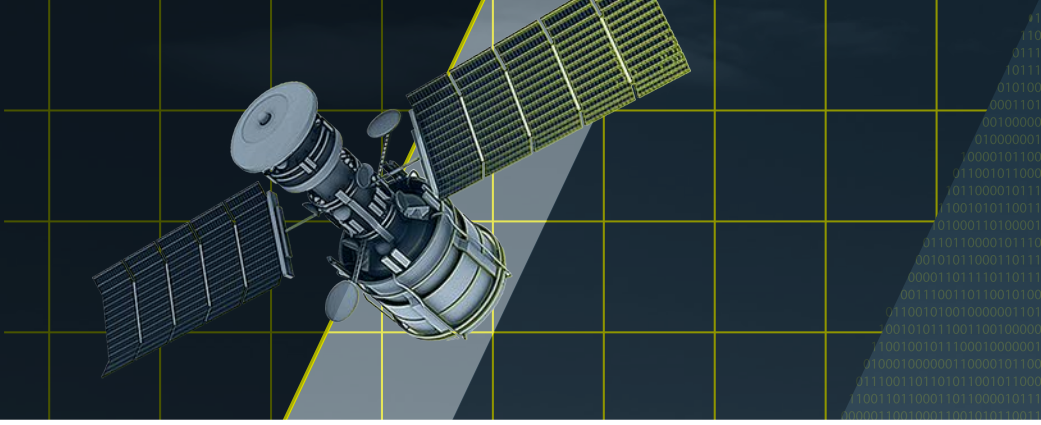
1. **Prioritize training investments for full-spectrum cyber training simulations, content, and ranges:** The complexity of cyberspace activities is like that of multi-flow dynamic combat clearance—it requires countless repetitions and TTP refinement to instill confidence in the operator's capability to execute the mission. Like combat clearance, cyber training needs to be integrated into training environments using physical hardware and software to depict adversary terrain as realistically as possible. For teams to fully integrate full-spectrum cyber capabilities across the SOF disciplines, operators need to witness them in action—like, for instance, the cyber manipulation of a target vessel during an interdiction operation or cyber destruction of an adversary surveillance system during direct action. SOCOM requires deliberate and continuous investment to enable SOF cyber operators to rapidly build the skillsets required for future mission success.

   Funded prioritized cyber training, aligned to SOF-peculiar operational planning requirements, makes the cyber domain applicable and valuable to SOF operator roles and mission requirements, and enables cyber to fully integrate (live, virtual, and constructive) into SOF training exercises. This would evolve SOF exercises from "white carding" cyber activities, to enabling operator use of friendly and adversarial cyber effects that are operationally relevant and realistic. For instance, exercises can leverage catalogs of the latest known vulnerabilities concerning networks, hardware, and software—and leading manufacturing capabilities can help put such capabilities into play. Exercising in this manner will build stronger connectivity and interoperability between SOF and CYBEROM cyber teams, resulting in more effective SOF-enabled cyber operations and cyber-enabled special operations. For example, realistic joint exercises will enable the cross pollination of SOF cyber and conventional cyber operations to develop shared practices and greater interdependence. SOF-peculiar exercise environments will also provide operators with a sandbox to experiment with innovative technologies like AI/ML to support forward-deployed operators who may only have minutes to integrate cyber tools into any given mission.

2. **Establish a SOF cyber indefinite delivery/indefinite quantity (IDIQ) program:** SOCOM and the service components are developing SOF-specific cyberspace requirements for training, exercises, and operational use. The force requires a program office and method to accelerate the acquisition, distribution, and sustainment of these unique capabilities. The traditional acquisition process cannot keep up with the rate of technological change for cyberspace, even with the Special Operations Forces Capabilities Integration and Development System (SOFCIDS). Teams need ready access to cyber industry subject-matter experts, innovative training programs, and cutting-edge tools to develop, test, and evaluate cyber capabilities that could be rendered ineffective by patching on any given day. Establishing a robust IDIQ at SOCOM would be the quickest and most efficient means of supporting the warfighter.

3. **Implement the SOF-Space-Cyber Triad:** The asymmetric advantage offered by integrating the unique capabilities of SOCOM, CYBERCOM, and U.S. Space Command (SPACECOM) will only be realized if cross-functional experiments and training drive a campaign of learning. The outcomes of such an effort will be better-defined use cases, increased speed, and operational agility. Critically, these joint efforts will also identify friction such as differences in doctrine, interpretation of authorities, and potential cultural challenges. An essential outcome is improved trust, a prerequisite to creating the cultural change required to optimize the potential of the triad. It is only through close collaboration and demonstration that the operators and front-line leaders will fully understand the cross-functional and cross-organizational capabilities for mission execution.

Immediately and effectively improving the training for SOF-cyber capabilities will better enable the full range of SOF missions on the future battlefield. One of SOCOM's **SOF Truths** states, "Competent special operations forces cannot be created after emergencies occur." This is also true for cyber forces and capabilities. Now is the time to refine and implement the doctrine, policy, organizations, capabilities, training, and resources required to improve SOF's success in competition, crisis, and conflict against all adversaries. Now is the time for SOCOM and the joint force to fully invest in bringing SOF cyber capabilities to the forefront of joint force operations.



THE FUTURE OF WARFIGHTING: INTEGRATED CYBER WEAPONS

Attaining overmatch in the cyber domain

As the Department of Defense (DOD) procures new cyber warfighting capabilities for an all-domain operating environment, the Joint Cyber Warfighting Architecture (JCWA) concept is adapting to achieve not just interoperability—the power to share data among all systems or core components of the joint architecture—but also true integration.

JCWA (as an architecture of systems) is designed to collect, fuse, and process data and intelligence to provide enhanced cyber capabilities ranging from situational awareness and battle management to training, exercises, mission rehearsals, joint fires, and common tools for warfighting missions.

The warfighting tools and services in this architecture are core to projecting combat power and mission readiness. Because of this, they require approaches in agile development that can be deployed more rapidly and with greater precision, with more advanced managed attribution techniques for operators, and approaches to information sharing that can more rapidly handle large volumes of unstructured data moving across domains and classifications.

Today, full-spectrum cyber operations must be integrated and synchronized across all domains. To prevail in future conflict, competition, and crises, the joint force must plan and execute full-spectrum cyber operations faster and more effectively than the enemy. Acquiring and employing the unique capabilities to achieve U.S. superiority in the cyber domain requires more than linking and maturing disparate legacy systems: The imperative is to create a hyper-integrated cyber weapons system that provides an enduring advantage over current and future threats.

As the JCWA program evolved from original concept to initial deployment over the past five years, adversary cyber capabilities have likewise aggressively evolved. This dynamic has created a need to deploy solutions faster and with greater agility to outpace emerging threats. Solutions must be constructed and delivered to meet specific mission needs at the threat and domain level, and systems must be able to simultaneously refactor data, tools, and solutions as targets evolve.

The need for this agile and lethal weapons system is reflected in DOD's strategic cyber goals: The joint force must achieve overmatch against the pacing challenge from China, the acute threat from Russia, and other persistent threats. All six JCWA components are crucial to achieve integrated deterrence, campaigning in and through cyberspace, and protecting global allies and partners. The Joint Common Access Platform (JCAP) component, for instance, will enable warfighters to project combat power in cyberspace while managing detection and attribution on a larger scale and with greater efficiency than legacy capabilities allow. This platform will need to include a full suite of tools and the ability to more rapidly respond to key operator challenges. Similarly, JCWA's cross-domain capabilities must evolve to handle rapid movement of large volumes of structured and unstructured data across multiple operator environments and varying classifications of environments.

THE WAY AHEAD

Evolve the baseline for requirements: The immediate challenge is propelling JCWA from its current state—the outcome of an initial attempt to acquire and field a cyberspace operations capability—to its future state: a fully integrated cyber weapons system accelerated by a partnership between the government and contractors who can demonstrate the rapid evolution of systems, utilization of new approaches for refactoring data, and extensive experience advancing information sharing across environments. Partnership with industry that provides for incentives and requires service-level agreements for outcome-based delivery against dynamic needs will provide alignment to the pace and complexity of the mission. Minimum viable solutions should be vetted in months, not years—and contractors should be utilizing parallel baselines, which mirror current delivery, to reduce risk. Contractors should be selected and maintained based on outcomes and responsiveness and held accountable for bringing the most current capabilities in the use of scalable and secure infrastructure across mission needs.

Take a data-first approach: All domain operations require secure, ubiquitous access to data across multiple disparate networks, including non-defense networks and weapons systems. Sensors and weapons systems must employ open data standards to optimize data flow and advanced analysis. Data is the ammunition that feeds the entire weapons system, enabling the rapid execution of critical missions with advanced cyber solutions tailored to meet current and emerging needs.

Achieve security by design: The platform must protect sensitive data in real time. Not unlike operators of software-centric 5G ecosystems, operators of the integrated cyber weapons system will need holistic protection that includes zero trust architecture (ZTA), continuous monitoring, development, security and operations (DevSecOps), and an expert workforce, as well as vulnerability research and embedded security. Analytics and automation, two of the seven pillars of zero trust, can be used to rapidly drive security improvements—policy updates aligned to the other pillars—over time at scale through the entire ZTA. The same mindset can also accelerate the growth of JCWA's arsenal. Just as the continuous development and deployment of new policies will be a critical enabler for secure and resilient cyberspace operations, so too must the next generation of JCWA harness the power of automation and DevSecOps to rapidly develop full-spectrum cyber capabilities at scale. These software-based warfighting capabilities would be tailored to meet a wide range of specific mission objectives.

"SUPERIOR STRATEGIC EFFECTS DEPEND ON THE ALIGNMENT OF OPERATIONS, CAPABILITIES, AND PROCESSES, AND THE SEAMLESS INTEGRATION OF INTELLIGENCE WITH OPERATIONS."

– CYBERCOM'S 2023 COMMAND CHALLENGE PROBLEM SET

Be intelligence-driven and threat-informed: JCWA component programs must be ready for tomorrow's cyber threats. Shadowing advanced threat activity via open-source and classified intelligence can help fill emerging knowledge gaps and sharpen the continuous development of JCWA's defensive and offensive capabilities. Also, JCWA programs can make greater use of operational insights on adversarial tactics, techniques, and procedures (TTPs), to include leveraging catalogs of the latest vulnerabilities concerning networks, hardware, and software. What's more, stakeholders have an opportunity to gain further insights as DOD increasingly incorporates contested cyber environments in exercises and training for conventional and special operations forces (SOF): Capturing lessons learned could help support the acquisition of operationally suitable and effective cyber capabilities.

Gain advantage in the cloud: As JCWA moves increasingly to hybrid cloud environments to enable data sharing and other functions, stakeholders must make this pivot an advantage rather than a liability. Obstacles to avoid when moving to the cloud include mission-workload migration pitfalls, vendor lock, and rising infrastructure costs. In short, to achieve the interoperability envisioned, JCWA must enable warfighting software developers to focus more on their core missions and less on the IT infrastructure. Imagine how missions would benefit if JCWA components made it as easy as possible for users to develop applications, migrate data and manage infrastructure across multiple cloud service providers. What's more, this data-driven weapons platform needs to be designed for real-time configuration management so the overall platform can rapidly reconfigure if one component changes.

Conquer cross-domain challenges: The software-enabled systems, sensors, and tools that make up the platform will need to incorporate novel ways of sharing data, enabling collective thinking, and distilling actionable insights, to include harnessing the power of data analytics and AI/ML. In short, JCWA must rapidly manage and access data across multiple platforms and classification domains. In fact, achieving permeability and agility across domains ranks among the top technical challenges for U.S. Cyber Command (CYBERCOM). JCWA systems will need to be designed and built to overcome three challenges that can impede the secure transfer of data across domains and among globally dispersed organizations:

- **Outdated data sharing processes:** Very often, missions require cross-domain data flows moving up or down classification levels—typically across U.S. government unclassified, secret, or top secret/sensitive compartmented information (TS/SCI) networks. Yet the cross-domain solutions (CDS) and guard technologies that facilitate information sharing are proprietary appliances that are not designed for the breadth of data types, volume of data, rapidly evolving mission/partner environments, or the speed of information sharing required by today's analysts and warfighters in evolving Joint All-Domain Command and Control (JADC2) environments. Also, many existing enterprise systems do not have a multi-level security (MLS) architecture to support data sharing, dissemination, and access to users with various security clearances and permissions.
- **Inability to meet AI's insatiable need for data:** AI/ML are essential for finding patterns, spotting anomalies, and moving toward predictive capabilities. However, enormous volumes of data are required to train and refine algorithms. That's in addition to information that must be centralized for cross-domain imperatives such as cybersecurity and JADC2. Also, analytic infrastructure solutions are needed to provide computing power for the development, training, and deployment of models/algorithms.
- **"One-off" software development:** Software developers across DOD have been overloaded with workflows requiring custom applications to be developed and deployed in a complex operational environment, each undergoing separate security accreditation and authority to operate (ATO) processes. Also, custom software solutions may not follow modernized software design patterns.

Enable global partners: The 2023 DOD Cyber Strategy highlights the strategic advantage and imperative of protecting and reinforcing the United States' global network of allies and partners. Increased collaboration with partners from industry and academia, foreign allies and partners, and interagency partners will bring significant advantages, and the future JCWA must address the challenges and opportunities presented by partner capabilities.

NEXT STEPS

Above all, JCWA platforms must be designed and developed with a clear focus on the operational needs of warfighters who will use the technology to execute crucial missions. Simply put, the joint force must be able to sense, understand, make decisions, act, and assess outcomes faster and more effectively than the enemy. Commanders must be able to see themselves, see the adversary, and see all other relevant actors, actions, and activities in the operations and information environments—all at mission-relevant speed. These "three sees" depend on secure and resilient networks, valid data, and predictable data flows. Here are a handful of recommendations for consideration:

- Design, build, test, and maintain JCWA components with the security and resilience needed to deliver suitable and effective cyberspace operations, even in a degraded state, when facing tomorrow's advanced unconventional threats. To understand and outpace emerging threats, take full advantage of open-source and classified intelligence, detection engineering, and reverse engineering.
- Evaluate JCWA components with mission-based cyber risk assessments that include detailed functional thread analyses of the attack surface mapped to missions, system functions, and potential cyber vulnerabilities where cyber risk ratings and priority levels are determined for each point of entry into the system's cyber boundary. Create attack-path vignettes describing potential operationally representative cyberattacks from source to target.
- Focus on dynamic infrastructure provisioning to meet evolving mission needs and provide high scalability, availability, resiliency, and disaster recovery to support software, cyber, and AI/ML workloads.
- Seek cross-domain solutions that are cloud-agnostic and provide an MLS solution, to include supporting connections to networks that link to networks at the tactical edge. Also, such solutions should enable bi-directional flows to support needs like DevSecOps, JADC2 mission planning, and intelligence collection. Using an open platform, build on government-owned off-the-shelf software can provide cost savings without vendor lock. In addition, a modular architecture can provide flexible, reusable components provide speed to mission, faster upgrades, and scalability for any complexity.
- Consider proven, accredited cross-domain solutions to support analysis of capabilities for national security missions. Such accreditations could include Top Secret and Below Interoperability (TSABI), integrated with National Cross Domain Strategy and Management Office (NCDSMO) Raise the Bar (RTB) compliant guards. Leverage use-case models and lessons learned to inform the approach for discovering, accessing, disseminating, and effectively sharing data.
- Use DevSecOps and machine learning operations (MLOps) to rapidly build, test, deploy, and operationalize capabilities at the speed of mission, including low-to-high (L2H) and high-to-low (H2L) delivery.

National security increasingly depends on full-spectrum cyber operations. Cyber forces need to uphold national defense, disrupt and dismantle emerging threats, and collaborate with international partners to advance shared goals in cyberspace. DOD and the industrial base have an unprecedented opportunity to make JCWA components a truly integrated weapons platform that is agile, scalable, interoperable, and resilient. Meeting these acquisition needs today will position the joint force to meet the operational needs of the nation tomorrow.

EMPOWER PEOPLE TO CHANGE THE WORLD®

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining more than 100 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: Empower People to Change the World℠.