OPERATIONS
WHITEPAPER

Peraton

ENSURING FREEDOM OF OPERATIONS IN THE CYBER CONTESTED SPACE DOMAIN

DO THE
CAN'T BE DONE.

EXECUTIVE SUMMARY

Organizational leaders are fast discovering how digital transformation benefits their mission critical programs and business processes. Multitasking remote workers are increasingly teaming virtually, any time and from anywhere, confidently and safely leveraging efficient cloud platforms to achieve timely results. Data scientists now apply AI/ML capabilities to swiftly discern actionable trends from oceans of collected data. Technologists exploit autonomous processes to streamline previously labor-intensive tasks. Watch standers respond decisively to enterprise threats revealed in real-time on single pane displays for hyper situational awareness. These and many other welcome transformations help enable modern work environments. However, they demand high performance from the organization's cyber and information technology professionals.

Chronic shortages of expert staff, burdensome upkeep of unsafe legacy infrastructure, and overtasked program managers with little bandwidth or resources to apply to new initiatives challenge even the most dedicated teams. Additionally, the need for reliability, resilience, and security has never been greater. The audacity of sophisticated cyber actors spying on sensitive programs, disrupting business processes, or extorting fees for ransomed data increases with every successful compromise. Still, the future is bright as we are in this together. Information sharing and cooperation among partners—federal, state, local and tribal governments, the private sector, academia, as well as our international allies—will be key to our mutual success in navigating the digital road ahead.

On May 12, 2021 the Biden administration issued a new executive order (EO)[1] to enhance our nation's cybersecurity posture which notably includes coordinating partnerships with the private sector to support the EO execution. The EO represents a significant number of activities that will require directed actions and significant effort significant effort among all U.S. federal government agencies and government contractors/subcontractors.

The new EO requirements make cybersecurity and securely managing government data more important than ever before. Peraton welcomes this opportunity to further our trusted partnership with the Federal Civilian Executive Branch (FCEB) agencies, Department of Defense (DOD), and the Intelligence Community (IC) in support of their mission accomplishment. This whitepaper highlights Peraton's capabilities that can directly enhance implementation of the EO.

A successful cyberattack directed against U.S. space systems and related infrastructure will have sever consequences for national security, the economy, as well as safety, and quality of life. Cyber effects on U.S. space systems can disrupt, deny, degrade, deceive, or destroy the space capabilities upon which the world has become increasingly dependent. The attack surface is growing exponentially larger as more spacecrafts connect with ground-based assets and users. When directed toward this attack surface, threat actor cyberattacks will accomplish their goals with low investment and minimal skill required.

Today's cyber operations require the capabilities for real-time threat detection and rapid, intelligent mitigation with autonomous prescribed courses of action. The development of such capabilities for the contested space domain is essential to combat emergent threats. Leveraging Security Orchestration and Automated Response (SOAR) technology, Artificial Intelligence, and Machine Learning (AI/ML), and advanced data analytics that can help the U.S. stay ahead of the adversary will drastically improve cybersecurity operations performance, resilience, and agility, as well as lower costs.

Peraton is poised to address full spectrum cyber activities targeting our space assets. This whitepaper presents a dynamic roadmap to realize the vision for freedom of operations in a cyber-contested space domain.

Underpinning the criticality for full spectrum protection is Space Policy Directive 5 which highlights that the U.S. and a mutually dependent world are increasingly reliant upon the space environment for communications, navigation, financial transactions, weather monitoring, security, and intelligence to support interdependent system-of-systems critical infrastructures whose disruption or destruction would generate lasting damage[3]. Additionally, Executive Order 14028 mandates that the DoD must meet or succeed the standards of prevention, detection, assessment, and remediation of cyber incidents[1].

With the continuous exposure of space systems to emergent cyber threats from nation state, terrorist, hacktivist, and criminal adversaries, there is a need for next-generation space enterprise protection spanning the space architecture components. Space systems, operations, development schedules, and budgets are often prioritized over cyber security during implementation and service delivery. When security is not prioritized it inevitably leads to significant cyber vulnerabilities in even the most well-architected systems. **Figure 1** illustrates the cyberattack surface for multi-segment space systems that emphasizes the ground segment[2].

Peraton's security in depth approach empowers the space industry to operate from a position of knowledge necessary to ensure freedom of operations in a cyber-contested space domain while meeting U.S. security requirements integrated with commercial best practices.

An essential problem space systems are encountering is transforming program architectures to incorporate a comprehensive cyber defense capability with end-to-end situational understanding of an adversary kill-chain to prevent lateral movement across space systems. Achieving this understanding necessitates leveraging the Agile concept of responsive, iterative development while incorporating development, security, and operations (DevSecOps) principles and applying Zero Trust Architecture (ZTA) design tenets to provide a continuous delivery pipeline for cybersecurity without impacting mission operations.

In full partnership with our customers, Peraton can tailor the advanced capabilities to enhance full-spectrum cyber operations for space systems to address the challenges and solutions summarized in **Figure 2** and subsequently explained in more detail.

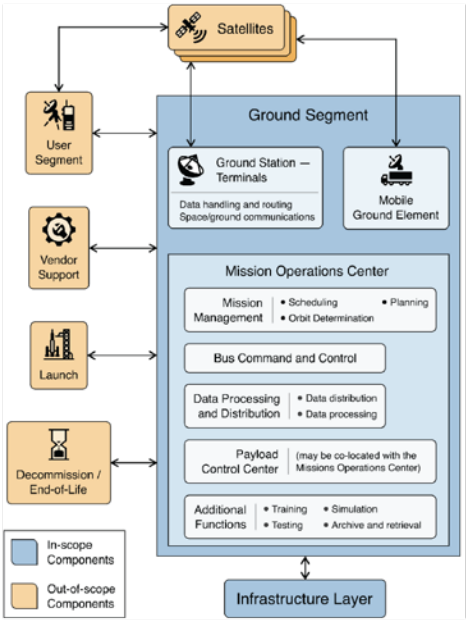

Figure 1: Space Architecture Components

CURRENT CHALLENGE	OBJECTIVE	CAPABILITY	KEY FEATURES
Mission risk cyberattack surface assessment	Planning and assessment	Deep Cyber Resiliency Assessment (DCRA)	ACE group assess mission vulnerability from the viewpoint of an adversary; this DCRA validates and develops exploits, mitigates, and continuously monitors to maintain compliant system security.

CURRENT CHALLENGE	NIST CSF	CAPABILITY	KEY FEATURES
Lack of space system visibility and situational awareness	Identify	ThreatBoard (TB)	TB provides the data fabric and tools to organize and mine large datasets, break down data silos, collaborate in real time, and enable enterprise analysis independent of event location.
Real-time detection of threats in space systems	Detect	CyberVAN for Space (CV4S)	CV4S delivers a high-fidelity network modeling and simulation testbed in a hybrid network emulation (HNE) platform for evaluating the performance and characteristics of hypothetical or actual networks.
Contextual analysis for actionable threat intelligence	Protect	Cyber Functional Artificial Intelligence (CyberFAI)	CyberFAI uses Artificial Intelligence/Machine Learning (AI/ML) and Heuristic Behavior Analytics (HBA) to identify patterns and anomalies amid noise based on MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and D3FEND frameworks.
Operationalize incident response	Respond	CyberFAI	Threat hunters identify the latest intrusion indicators and tactics while cyber forensic analysts' reverse-engineer detected exploits, sharing relevant knowledge with their mission partners.
Rapid secure software development	Recover	Transformation Factory (TF)	TF provides a rapid application development pipeline fed by various data streams to meet mission needs without impacting operational timelines.

Figure 2: Current challenges and solutions

PLANNING & ASSESSMENT

Deep Cyber Resiliency Assessment (DCRA)

Without a complete understanding of space system cyber vulnerabilities, effective threat mitigation is an unachievable task. A Deep Cyber Resiliency Analysis (DCRA) provides customers with the means to identify and remedy potential exploits in three phases. Phase 1 is an Attack Path Analysis (APA) that provides the framework for determining the major faults within customer networks by examining them from an adversary's perspective. Red teams conduct penetration testing in Phase 2 to find the most likely enemy attack vectors and recommend remedial courses of action. Phase 3 is risk mitigation that can be done via exercises to allow for realistic scenarios in which to wargame responses against simulated threat actors and mitigate risk. Through this practice, customers gain an understanding of the enemy's tactics to enable updated standard operating procedures to make friendly networks more defensible.

The DCRA developed by the Advanced Cyber Effects (ACE) Group has provided customers with the battlefield edge by painting an accurate picture of adversary space systems utilizing multiple data feeds filtered into contextualized threat intel. This allows for numerous potential overmatches when applied to the analysis of enemy cyber capabilities, namely the detection of vulnerabilities to penetrate air-gapped networks, assisting in the building of zero-day effects, and exploitation of standard aerospace protocols.

When evaluating friendly systems, the resolution of vulnerabilities found by the ACE Group during their assessment has resulted in a 60-80% reduction of attack surface area in as little as one month compared to only ~5% from system scans alone. Combining the mitigation of enemy attack vectors with the detection of novel adversary exploits provides a significant competitive advantage.

IDENTIFY

ThreatBoard (TB)

With a demonstrated deficit in qualified cyber professionals in the workforce, now more than ever, space cyber analysts and threat hunters need solutions that help them keep pace with the evolving threat landscape. Protecting national security in the face of cyber threats posed by modern adversaries requires new thinking. At the core of the challenge is a lack of awareness of the millions of data streams that move into and around organizations daily. Without this visibility and the ability to correlate internal and external events it is nearly impossible to identify new threats, address undetected events, or develop effective defenses against the entire threat landscape.

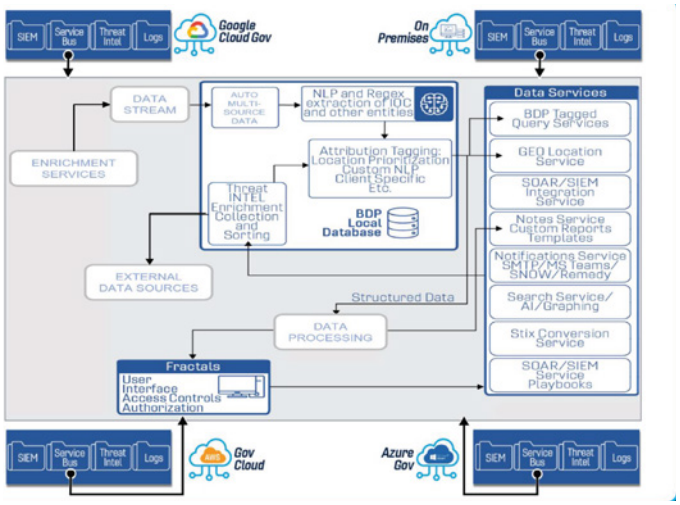

Figure 3: ThreatBoard (TB)

ThreatBoard's (TB) threat management platform depicted in Figure 3 is a way for customers to integrate any cyber event data source, regardless of format, into a single consolidated data repository for enrichment and enhancement of threat information. This eliminates silos and makes data accessible to parse, correlate, research, and act upon at machine speed. Integrating all data from critical space infrastructure informs and enriches situational awareness and provides the foundation of a proper response. This solution permits dynamic search capabilities across satellite constellations and ground station networks and allows for data scalability with secure integrated AI/ML threat detection.

On-premises edge sensors perform rapid response of known cyber threats and forwards results to cloud computing systems for AI/ML trend analysis, correlation, and unknown cyber threat detection across the space ecosystem reducing risk and increasing time between threat detection and rapid response. In effect, ThreatBoard alleviates cyber workforce challenges, enabling cyber responders to do more at every level while reducing their workload.

DETECT

CyberVAN for Space (CV4S)

Cyberresiliency is a growing and unmet requirement in many of the new commercial and DoD space architectures being assessed by the U.S. Space Force (USSF). In terms of cyber protection, space systems rarely get the funding and development needed to be secure. With the clear expansion of customer systems and the integration of systems across all warfighting domains the importance of space cyber systems will continue to grow.

The testing sandbox depicted in **Figure 4** allows testing and evaluation of space system integrity and cyber resiliency. This simulated environment creates a safe model to replicate and employ threats at scale, either pre-planned or in real-time. It also enables mission planners or white teams to design and execute missions with an intuitive graphical user interface, record/playback scenarios, and export time-sequenced scenario data for further analysis. Proposed software and hardware upgrades then undergo testing prior to integration in the mission system. This allows engineers to learn from realistic performance analysis prior to implementation.

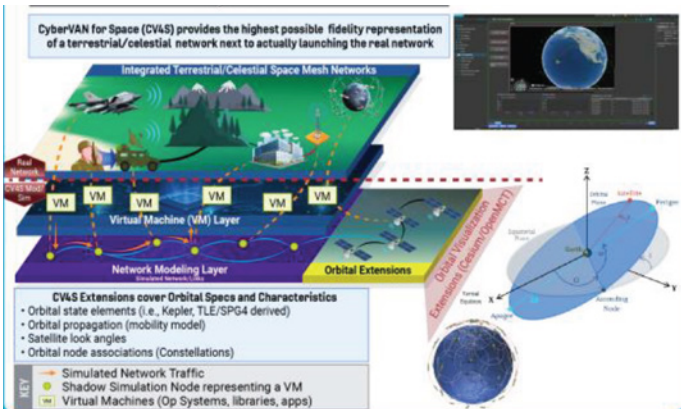

Figure 4: CyberVAN for Space (CV4S)

Cyber VAN for Space (CV4S) provides a realistic, high-fidelity cyber environment that scales to handle large networks, incorporates wired and wireless networking effects accurately, and provides flexible, easy-to-use libraries and interfaces for users. This cyber Virtual Assured Network (VAN) environment provides realistic modeling of large virtual and physical networks, including enterprise, military, and hybrid networks. CV4S's fundamental innovation is its transparent forwarding capability, which enables the seamless forwarding of traffic originating on virtual machines (VMs) through a simulated network to destination VMs. This enables a high-fidelity representation of terrestrial-based satellite control stations and system-agnostic space-based systems possible.

PROTECT AND RESPOND

Cyber Functional Artificial Intelligence (CyberFAI)

Peraton has demonstrated the value of incorporating AI/ML and AR/VR tools by providing new ways to visualize the threats data flow, as well as a new method to extend support for collaborative incident response. Automated decision support tools quickly present cyber threat indicators to analysts. This data sensing process is rapidly adaptable to complex operating environments and provides fast, dynamic detection and mitigation of continuously evolving cyber threats. Software-defined data sensing will help protect space systems that no longer have a traditional network perimeter by shifting from a net-centric approach to a data-centric one. Data-centric perimeters minimize impacts to the existing networks. The application of AI/ML, AR/VR tools, and automated decision support tools support the data centric perimeters and protect space systems.

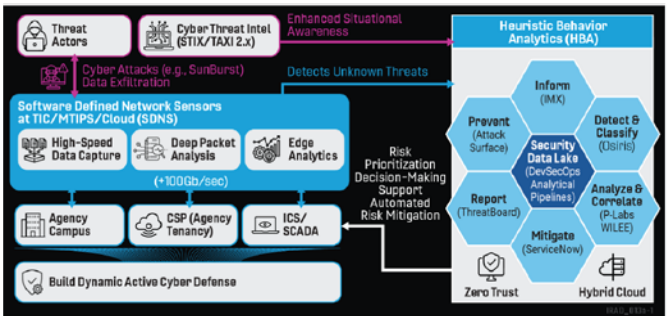

Figure 5: Cyber Functional Artificial Intelligence (CyberFAI) Architecture

As seen in **Figure 5**, CyberFAI is a next-generation space cyber ecosystem that enables real-time network telemetry ingestion, threat detection, and analysis with cyber remediation to protect and respond at the speed of attack.

CyberFAI is an AI/ML capability consisting of four tiers: Sensing, Profiling, Cognitive Sense-Making, and Response Automation. The data sensing capability helps classify adversary intent early in the attack cycle by incorporating a software-defined detection model. Peraton can quickly design and deploy a hybrid sensor module with risk mitigation playbooks based on customers' network, operations, classification level, and requirements. This approach scales to the mission and results in actionable intelligence.

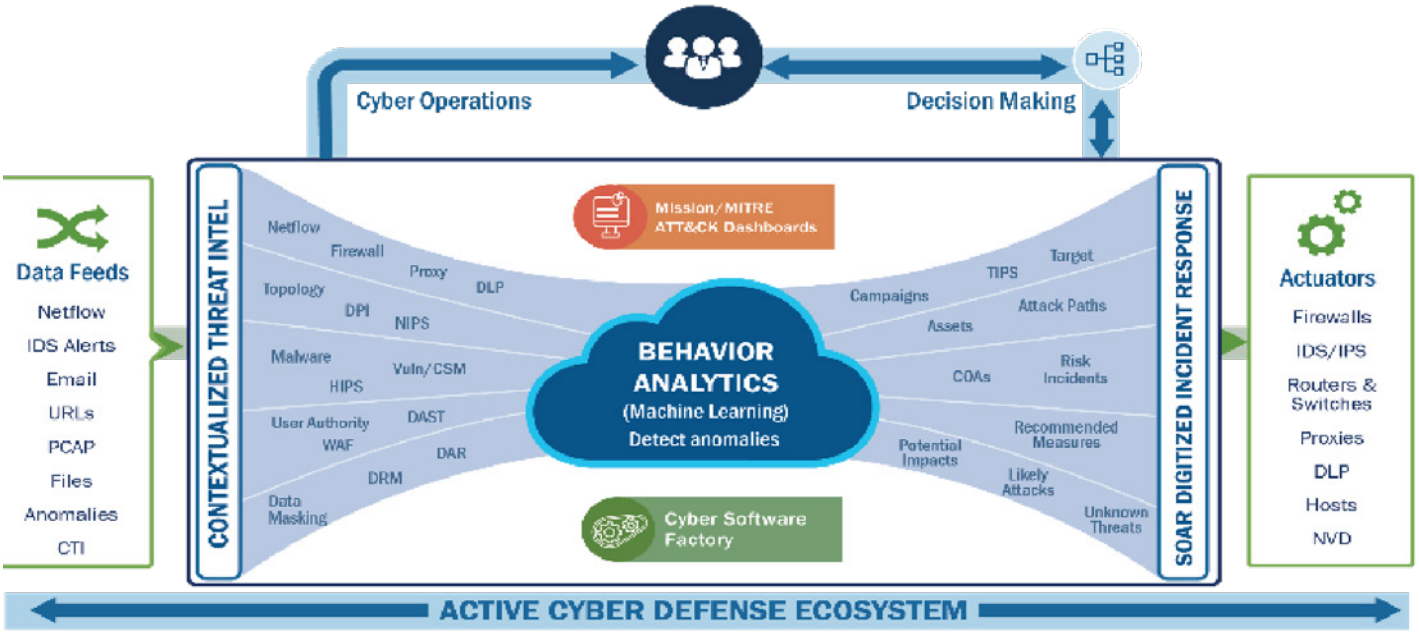

Figure 6: Heuristic Behavior Analysis (HBA)

Peraton's Heuristic Behavior Analytics (HBA) depicted in Figure 6 is an advanced data management and collaboration framework that combines tactical, operational, and strategic intelligence in context with event correlation to improve situational awareness. The HBA centralizes security information and event collection, as well as learns from every operation to reduce future false alerts. Events trigger cognitive reasoning components that alert and generate predictive operational intelligence and automate space network defense response. Decision-makers stay continuously informed with context to manage risks as circumstances evolve. Capturing and preserving context ensures threat analysts acquire timely insight from events occurring across the space systems infrastructure.

RECOVER

Transformation Factory (TF)

For operations to continue unimpeded following a cyberattack, it is crucial to create backup work products while also modifying tools to prevent similar attacks in the future.

The Transformation Factory (TF) will accelerate space industry organization's ability to rapidly deliver relevant value by honing knowledge, experience, deployment speed, code quality, and security. Utilizing Agile and DevSecOps methodologies, Peraton builds security into software at every lifecycle stage. This approach reduces rework and the risk of security vulnerabilities in production environments, speeding up Authorization to Operate (ATO).

The TF seen in **Figure 7** is a best-of-breed integrated collection of tools, data, and processes operating across on premises or hybrid cloud environments. TF leverages Agile and DevSecOps principles as well as best practices from government, industry, and academia, resulting in collaborative applications for cyber operations that builds security into software at every lifecycle stage. The TF optimizes processes with the use of automation to ensure accelerated delivery in a secure manner. This not only adds inherent protection from the development of a high-quality product but does so at a lower cost and in a shorter timespan than traditional methods.

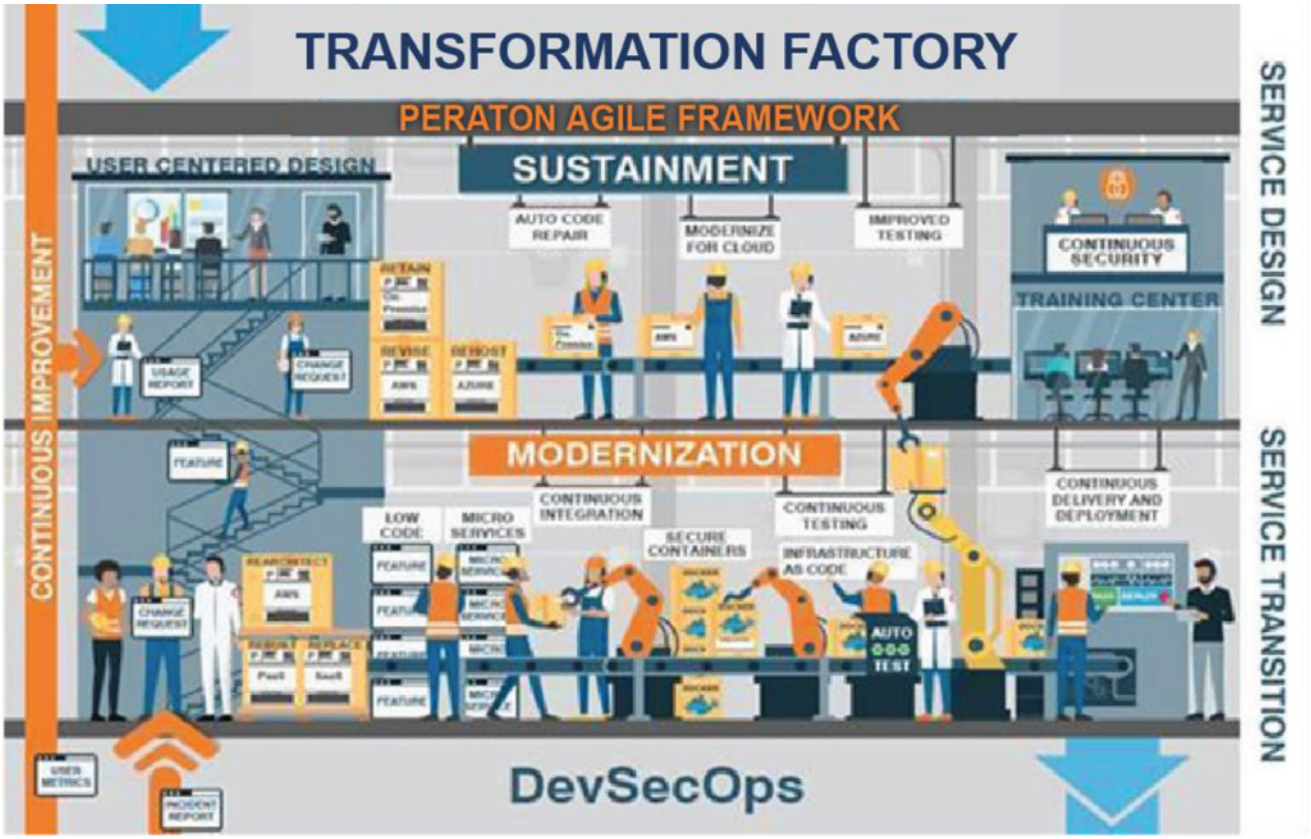

Figure 7: Transformation Factory (TF)

FUTURE CAPABILITIES AND PARTNERSHIP

As the nation's reliance on space systems continues to increase, it becomes even more urgent to defend this critical infrastructure and respond in a timely manner to a growing number of threat actors.

There is no single solution because cybersecurity threats and technologies evolve quickly, demanding a dynamic roadmap approach as discussed in this white paper to ensure freedom of operations in the cyber-contested space domain now and into the future. The approach can completely answer the NIST Cybersecurity Framework recommendations to defend space systems and assets as desired by customers.

For further information and to schedule a demonstration, please contact Peraton Director Space Cybersecurity Growth Scott Sage at ssage@peraton.com.

Resources

[1] Executive Order on Improving the Nation's Cybersecurity." The White House, 12 May 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[2] "Presidential Policy Directive -- Critical Infrastructure Security and Resilience." National Archives and Records Administration, National Archives and Records Administration, 13 Feb. 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[3] Lightman, Suzanne, et al. "Satellite Ground Segment – NIST 8401." Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control, NIST, 18 Apr. 2022, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.pdf.

ABOUT PERATON

Peraton drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As the world's leading mission capability integrator and transformative enterprise IT provider, we deliver trusted and highly differentiated national security solutions and technologies that keep people safe and secure. Peraton serves as a valued partner to essential government agencies across the intelligence, space, cyber, defense, citizen security, health, and state and local markets. Every day, our employees do the can't be done, solving the most daunting challenges facing our customers.

© 2023 Peraton