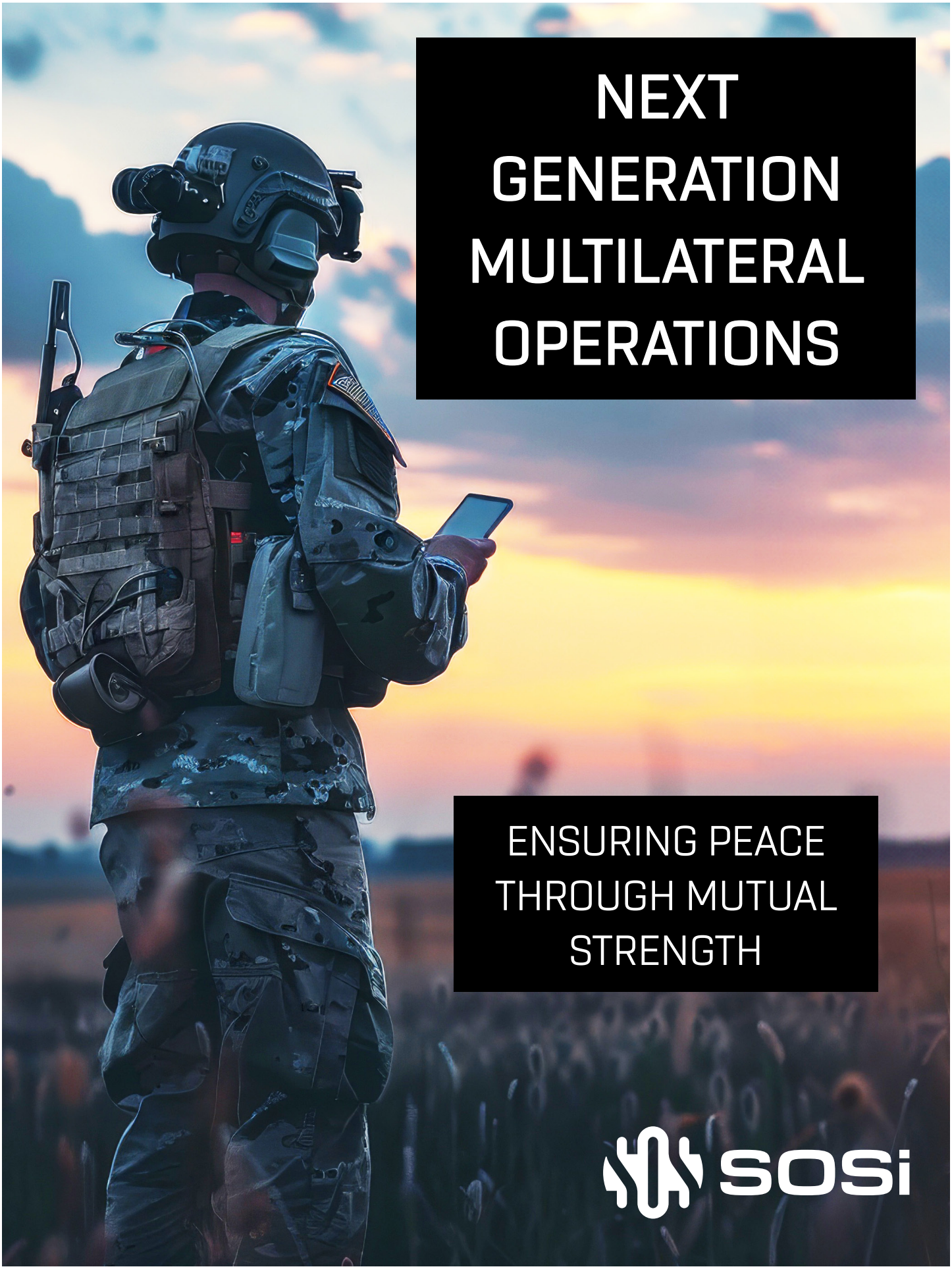
NEXT GENERATION MULTILATERAL OPERATIONS
ENSURING PEACE THROUGH MUTUAL STRENGTH
SOSi

Next Generation Multilateral Operations

Ensuring Peace Through Mutual Strength

As the Department of Defense (DoD) continues to adapt to evolving global challenges posed by the Great Power Competition (GPC), there is an increasing emphasis on agile, multilateral, and data-dominant operations across all theaters. Specifically, the Indo-Pacific's distinct characteristics — its vast operating environment, geographically dispersed warfighter presence, and rapidly evolving mission requirements — present unique challenges and opportunities for implementing advanced digital infrastructure.

The solutions to these challenges must allow for advanced computing such as AI/ML at the tactical edge; resilient architectures to robustly accommodate Denied, Disconnected, Intermittent, and Limited (DDIL) conditions; and agile data protection and access control supporting the region's unique complexity.

SOSi has proudly supported coalition communication missions for INDOPACOM and other COCOMs for more than two decades. We believe the following four focus areas are critical to best posture the U.S. and its coalition partners for the evolving activities in the Indo-Pacific theater:

1. Forge a Resilient, Agile Talent Pipeline
2. Achieve Data Dominance at the Tactical Edge
3. Build Resilient Infrastructure
4. Enable Agile Multilateral Communications

Forge a Resilient, Agile Talent Pipeline

In the rapidly evolving landscape of the Indo-Pacific theater, the human element remains paramount. The complexity of multilateral operations, coupled with the integration of cutting-edge technologies, demands a workforce that is not only skilled but also highly adaptable. However, significant challenges in workforce development must be addressed to ensure operational success.

The accelerating march of innovation has created a substantial gap between required and available skills, with personnel shortages demanding that military personnel frequently take on unfamiliar roles while juggling multiple responsibilities. The dynamic nature of threats in the region further necessitates a workforce capable of continuous learning and adaptation.

Addressing these challenges requires a multi-faceted approach. A comprehensive workforce assessment is crucial to identify skills gaps and training needs. Enhanced, ongoing training programs should cover not only technical skills,

but also adaptability, critical thinking, and cross-cultural communication. Leveraging public-private partnerships can rapidly integrate cutting-edge skills and technologies, while fostering a culture of innovation within the workforce. Providing opportunities for cross-functional exposure can also build a more versatile and resilient talent pool.

Likewise, targeted collaborative relationships with universities can create a pipeline for a future workforce. These partnerships would aim to align information technology, cybersecurity, software development, and engineering curricula with real-world best practices and practical applications.

However, current DoD workforce standards — such as DODD 8570 and 8140 — do not sufficiently address the evolving workforce needs in the Indo-Pacific theater. To close this gap, a more comprehensive strategy is required. Close collaboration with critical vendors is essential to familiarize key stakeholders with industry best practices. This partnership approach enables the certification of experts on essential tools and maintains strong vendor relationships, allowing for rapid issue resolution and collaborative problem-solving when facing new challenges.

SOSi, for example, actively collaborates with the Linux Foundation and the Open Source Security Foundation (OSSF) to keep our workforce at the forefront of open-source software development, ensure our experts are certified in the latest security best practices, and leverage extensive resources to address emerging challenges and foster collaborative innovation.

SOSi's experience in supporting coalition communication missions for INDOPACOM and other COCOMs illustrates the effectiveness of these strategies. Our approach to workforce development, emphasizing continuous learning and adaptability, has been instrumental in successfully implementing complex systems like the USINDOPACOM Mission Partner Environment (MPE).

By combining these strategies, it's possible to create a more robust, adaptable, and skilled workforce capable of meeting the unique challenges of the Indo-Pacific theater.

KEY RECOMMENDATIONS

- Industry and Government co-invest in workforce upforce skilling

- Perform skill assessments of critical techniques and technologies relevant for Indo-Pacific operations

- Enhance strategic talent plans that include a mix of workforce training, workforce exchange programs such as OSD's Public-Private Talent Experience (PPTE).

- Increase engagement with commercial best practice organizations such as Linux Foundation and OSSF to inform talent strategy.

Achieve Data Dominance at the Tactical Edge

Achieving data dominance at the tactical edge has become a cornerstone of operational success. This shift demands a transformation in how we approach data processing, storage, and analysis, particularly in environments where connectivity is unreliable or compromised. By leveraging distributed architectures and advanced AI/ML capabilities, military forces can enhance their ability to make informed decisions rapidly, even in the most challenging conditions. The transition from datacenter-centric models to distributed systems, coupled with tailored AI/ML solutions for DDIL environments offers a path to significantly boost operational effectiveness and resilience across the spectrum of military operations.

Moving from Datacenter-Centric to Distributed Architectures

The vast and diverse operating environment of the Indo-Pacific region necessitates a shift from traditional datacenter-centric models to more distributed architectures. Current coalition networks rely heavily on thin or zero client solutions that perform most computing tasks back at a centralized datacenter. This model, however, presents significant limitations for enabling robust computing AI/ML capabilities at the edge and providing advanced workloads like AI/ML resilience to DDIL conditions in the face of advanced threat actors.

The solution to these challenges lies

in moving toward cloud-native technologies and distributing "tactical" data centers. This approach brings computing power closer to where it's needed most, enhancing operational capabilities and resilience.

The INDOPACOM Mission Network (IMN) exemplifies this approach by incorporating cloud-native design principles within its on-premises private cloud infrastructure. While currently operating as an on-premises solution, the IMN's architecture is built with cloud-native concepts, utilizing technologies such as Kubernetes and Istio. This forward-thinking design creates a flexible and scalable infrastructure that aligns with commercial best practices.

Although not yet integrated with commercial or government cloud services, this architecture positions the IMN for potential future expansion. The current design allows services to securely and automatically scale within the existing infrastructure, from large facilities on major islands to smaller, distributed processing centers on tactical assets or forward locations. This level of flexibility enables rapid response to emerging threats and changing operational needs across the region's varied landscapes and maritime expanses, while also facilitating a smoother transition to cloud or hybrid cloud environments when the government is ready to make that leap.

"We're not breaking away from protecting the data in the data center," SOSi Senior Network Subject Matter Expert John Netterwald said. "We're evolving the model to make data more accessible so our systems can continue to function effectively even when robust access to data centers isn't available."

Netterwald said that by distributing command and control nodes, the system enables the ability to communicate, process information, and act autonomously if main communication lines are compromised. This approach also emphasizes the need for diverse connectivity options. By integrating commercial infrastructure alongside military networks, it becomes possible to leverage any available communication channel in theater securely, enhancing overall resilience and flexibility.

This cloud-native design ensures cyber resilience while bringing compute and storage capabilities closer to the frontline. It maintains operational effectiveness even in challenging environments by allowing for rapid scaling and adaptation to changing conditions. The result is a significant enhancement in the capabilities of forces operating in the Indo-Pacific theater, providing them with the agility and resilience needed to meet evolving challenges.

AI/ML for DDIL Environments

Artificial Intelligence and Machine Learning are revolutionizing military operations, but their application in DDIL environments present unique challenges. While data dominance is integral for success in accommodating the GPC, achieving this in DDIL conditions requires innovative approaches to AI/ML deployment.

Traditional AI/ML models often rely on substantial infrastructure confined to a few global locations due to exorbitant costs. However, the Indo-Pacific theater demands a more flexible solution. The challenge lies in developing AI/ML systems that can operate across a spectrum of devices — from advanced models in large data centers to smaller military facilities, and down to tactical components at the edge.

In DDIL scenarios, when connectivity to larger resources is lost, models must adapt to this shift in available computing power. Moreover, limited transport infrastructure often makes it impractical to transmit large datasets back to central data centers for processing. The solution is to bring processing capabilities to the edge, enabling analysis on more modest devices in the field.

To address these challenges, a multi-tiered approach to AI/ML deployment is necessary. This involves creating an infrastructure that can seamlessly transition between large foundational models operating in secure regions and smaller, open-source models tuned for tactical hardware. By implementing MLOps (Machine Learning Operations) practices, for example, SOSi can automate the deployment and monitoring of ML workloads across this diverse ecosystem.

This adaptive AI/ML framework enhances situational awareness and decision-making speed at the tactical edge, even when connection to central command is limited or unavailable. It allows for real-time processing of vast amounts of information, transforming raw data into actionable insights rapidly.

KEY RECOMMENDATIONS

- Accelerate the evolution to cloud native to allow for workloads to scale seamless from tactical edge to strategic data centers

- Implement MLOps to enable flexible deployment of advanced AI/ML workloads to effective operate between tactical edge to strategic data centers

Build Resilient Infrastructure

The vast Indo-Pacific theater presents unique communication challenges that require augmenting traditional Defense Information Systems Agency (DISA) communication lines with cutting-edge commercial technologies. Leveraging all available communication paths in the region could provide over 100x the combined DISA capacity with over 50x additional connectivity points, greatly enhancing operational effectiveness, robustness, and resiliency of connectivity for military

forces.

To achieve this enhanced connectivity, the expansion of DoD Reference Architecture-based Cloud Native Access Points (CNAPs) and Commercial Solutions for Classified (CSfC) is critical. These approaches enable low-risk, secure integration of commercial technologies into military communications infrastructure. This integration can be implemented in several key areas:

Tactically Relevant Commercial Fiber and Cloud Transport
By leveraging commercial fiber-optic networks and cloud-based transport solutions, military forces can significantly increase their data transmission capabilities.

Commercial Low Earth Orbit (LEO) Satellite Constellations
The deployment of LEO satellite networks offers a game-changing solution for ensuring connectivity in remote and maritime areas of the Indo-Pacific. These constellations provide lower latency and higher bandwidth compared to traditional satellite communications, enhancing the military's ability to operate effectively across vast distances.

Expanded Private 5G Pilots
There is a growing opportunity to demonstrate secure communication options using both U.S. commercial and Partner Nation 5G infrastructure. By expanding private 5G pilots, forces can achieve high-speed, low-latency communications while maintaining necessary security protocols. This approach not only enhances military capabilities but also strengthens technological cooperation with regional allies.

Combining these commercial solutions with existing military systems — and developing protocols for seamless switching between them and military networks — will create a more robust, flexible infrastructure that would improve uninterrupted communication.

Preparing for Post-Quantum Cryptography
The looming threat of quantum computing to current cryptographic standards demands proactive measures. As quantum computers advance, they could break many encryption methods currently protecting sensitive military and government communications, potentially compromising national security. The threat of adversaries storing encrypted data now to decrypt later with quantum computers further exacerbates this risk.

To mitigate quantum computing threats, innovative approaches to post-quantum cryptography (PQC) are being explored for mission-critical systems in the Indo-Pacific theater. These efforts involve designing flexible and agile cryptographic architectures that integrate quantum-resistant algorithms with existing MPE and IMN systems. Crypto agility will be essential in future theater operations to accommodate rapid adaptation of systems to new cryptographic standards and threats without extensive overhauls, maintaining resilient and effective encryption.

Both symmetric and asymmetric cryptographic methods are being employed to provide robust security. The NSA deems symmetric encryption essential for high-security applications, while asymmetric solutions are also being explored for comprehensive protection.

These initiatives align with the National Security Memorandum 10 (NSM-10) mandate, emphasizing the need for quantum-resistant cryptography. By incorporating best practices from both NSA and NIST quantum cryptographic guidance, these efforts aim to bridge the gap with agile solutions that meet the highest security standards.

As an example of ongoing progress in this area, SOSi is piloting PQC solutions for the USINDOPACOM mission in collaboration with key technology partners like Arqit. Such partnerships demonstrate the potential for industry collaboration in developing and implementing advanced cryptographic solutions to address emerging quantum threats in the Indo-Pacific theater.

KEY RECOMMENDATIONS

- Accelerate pilots of diversified commercial transport solutions into war fighting networks to enable flexible, effective, and resilient operations

- Perform PQC pilots to mitigate threats from store and decrypt

Enable Agile Multilateral Communications

While updates and advancements to existing infrastructure are essential, equal attention must be given to the data flowing through these systems. The sophisticated communication networks in the Indo-Pacific theater support the movement and processing of vast amounts of sensitive information, but the true value lies in how this data is secured, shared, and utilized across the region's complex operational landscape.

The Indo-Pacific theater presents complex security requirements that extend beyond physical and digital infrastructure. These requirements necessitate seamless integration with diverse regional allies and partners, each with their own technological capabilities and security protocols.

While the need for interoperability is not unique to this region, the Indo-Pacific's geopolitical complexity and rapid technological advancement demand a particularly nuanced approach to building complementary security systems. These systems must be capable of adapting to evolving technology architectures

and policy frameworks, ensuring that the data flowing through advanced networks remains secure and accessible to authorized partners across the theater of operations.

A critical first step is establishing recognized standards within U.S. systems to address internal interoperability issues. For instance, streamlining communication between EUCOM and INDOPACOM systems will set the foundation for broader Combined Joint All-Domain Command and Control (CJADC2) initiatives and more effective collaboration with allies.

Importantly, there has been a paradigm shift in how security is approached within these systems. Previously, the focus was on net-centric domains, where each 'enclave' was secured and access to that environment was protected. However, this model has proven insufficient in the face of increasingly complex and distributed operations.

The DoD and its partners are now moving toward a model of information domains, emphasizing data-centric security. In this approach, data is tagged with unique sensitivities, enabling granular, need-to-know access control — regardless of where the information resides. This method ensures that sensitive data remains protected throughout its lifecycle, whether it's at rest in a secure datacenter or in transit across various networks and devices.

This data-centric security model, verified through Zero Trust architecture, ensures continuous protection of sensitive information while facilitating necessary coalition information sharing. Focusing on securing the data itself — rather than just the networks it travels on — provides a more flexible, resilient, and interoperable security framework.

Key challenges in this multilateral environment are multifaceted and complex. Federated identity management entails aligning authentication standards across organizational boundaries, a task complicated by varying national and institutional protocols. Coordinating data tagging taxonomies and information release policies becomes increasingly difficult as each partner organization often has its own unique approach to data ownership and classification. This diversity in data policies significantly complicates integration efforts, as reconciling these disparate systems requires careful negotiation and technical finesse. Furthermore, ensuring secure connectivity across various transport layers (satellite, commercial 5G, etc.) without compromising performance presents additional hurdles. The challenge is not just technical but also operational, as each of these aspects must be addressed while maintaining the agility and responsiveness required in dynamic theater operations.

SOSi and its INDOPACOM customers are actively engaging with nations like Japan and Australia to align on foundational elements such as federated identity and data tagging standards. This collaboration aims to create an interconnected, secure environment that respects each nation's unique cybersecurity journey while advancing towards a resilient, interoperable framework across the region.

KEY RECOMMENDATIONS

- Accelerate shift from network security domains to information domains

- Deepen collaborations across partner nations and cocoms to align on critical technologies such as federated identity attributes and data tagging standards

Conclusion

The Indo-Pacific theater demands innovative solutions in workforce development, data management, infrastructure resilience, and multilateral communications. Addressing these challenges requires a multifaceted approach: forging an agile talent pipeline, achieving data dominance at the tactical edge, building resilient infrastructure, and enabling agile multilateral communications. The shift towards distributed architectures, integration of commercial technologies, and adoption of Zero Trust principles are crucial steps in this evolution.

As the region's geopolitical landscape continues to evolve, the ability to adapt and collaborate across national boundaries will be paramount. By focusing on these key areas and leveraging public-private partnerships, the U.S. and its allies can enhance their operational effectiveness and maintain strategic advantage in this critical region.

SOSi

ABOUT SOSi

SOSi's core mission is to promote and protect the interests of the U.S. and its allies around the world.

Since our founding in 1989, we have empowered our employees to develop solutions that break through barriers, inspire innovation, and build resiliency. Today, our motto of "Challenge Accepted®" resonates through our work modernizing and securing legacy government IT systems, driving innovation for the U.S. Department of Defense and Intelligence Community, managing critical government facilities and infrastructure, delivering critical intelligence analysis, and supporting enforcement, humanitarian, and asylum operations at the border.

Yet, what sets SOSi apart is not what we do, but who we are. Our creative and spontaneous culture enables us to be bold, act fast, own and take responsibility for our results, and build and maintain relationships that matter. SOSi offers the depth, breadth, and infrastructure required for the most complex missions, coupled with the agility and innovation modern mission challenges demand.

Contact Us
www.sosi.com