Defence | White paper

CALIAN®
Confidence. Engineered.

Managing Operations in Contested Electronic Environments

Spectrum Superiority in the Modern Operating Environment

Summary

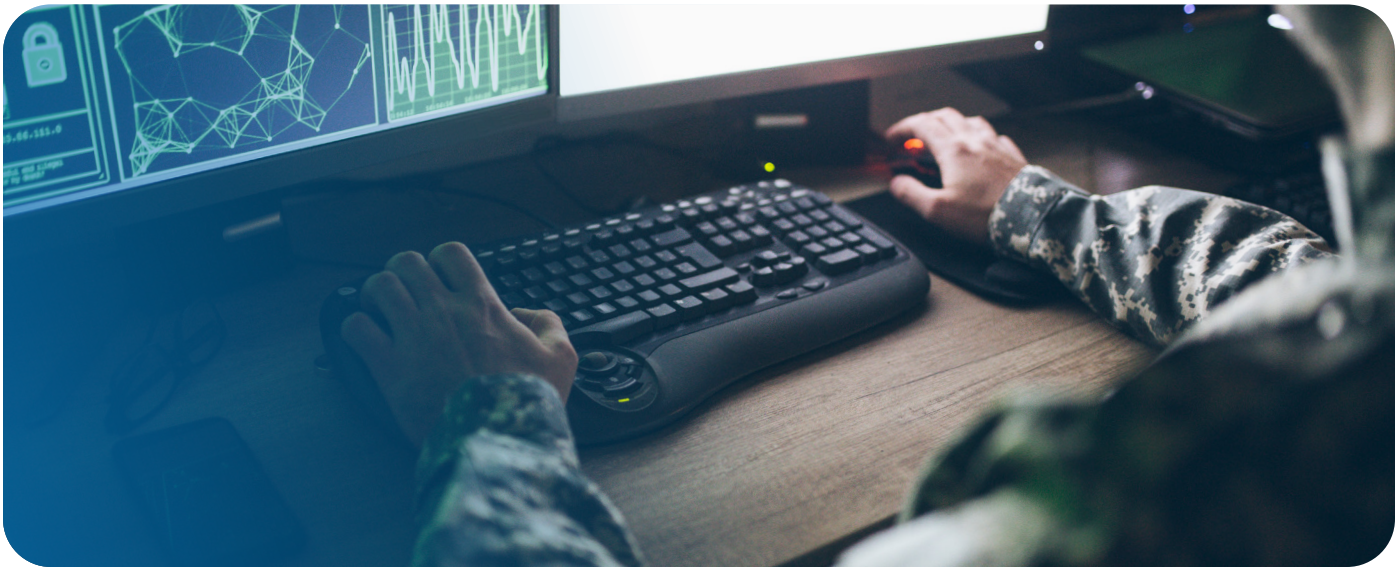
War in Ukraine is showing that the electro-magnetic spectrum is a domain of immense competition, including drones and UAVs, electronic warfare and emissions security. Maintaining an advantage in the electromagnetic spectrum is essential for digital and operational mobility. The electronic and computational advantage that Western countries assumed during decades of counter-insurgency cannot be assumed in the modern operating environment. There is a struggle for spectrum superiority, which means Western militaries need the means to protect platforms, devices, infrastructure and installations against unauthorized access to electronic data.

Operating in a Digital Environment

Electronic emissions are central to the modern battlefield. The increased use of small UAVs has changed battlefield surveillance, information flows and the ability to deliver precision fires against individual targets. Accordingly, emitters of electromagnetic energy—from radars and sensors to single operators of small UAVs—are becoming priority targets in an environment with overlapping sensors, emitters and the electronic warfare tools that seek to detect and jam adversary activity.[1] There is an "arms race" going on, pitting operators of UAVs and other systems that rely on wireless transmission against those jamming transmissions.[2] Each side is trying to use the electromagnetic spectrum for its advantage, while trying to deny their adversaries use of the same.

The electromagnetic spectrum challenge extends beyond the battlefield. Russian GPS jamming has been a regular trend, impacting civil aviation flights over Norway and Finland, reducing positional accuracy readings in the cockpit and risking commercial flights flying too close together.[3] Attacks on ground-based space infrastructure in 2022 significantly impacted satellite communication service, knocking over 100,000 communications customers out of service and shutting down 5,800 wind turbines, with major knock-on effects on power generation.[4] Space systems are vital infrastructure that connect more of daily life than many people appreciate. The banking system, in-dashboard GPS, cell-phone connectivity and global internet access, air traffic control, weather forecasting, and so much more, are dependent on reliable space-based systems, including ground infrastructure.

With threats of military action and threats to critical infrastructure, government and industry both need secure, reliable use of the electromagnetic spectrum. This means taking the necessary measures to reduce the risk exposure to jamming and unauthorized electronic intrusion.



Building Resilience Against Electronic Operations

Resilience is about avoiding and reducing risks wherever possible and taking the appropriate measures to manage the risks that cannot be avoided. Resilience in the electromagnetic spectrum requires hardening systems, components, facilities and networks against electromagnetic intrusion and interference, conducting real-time monitoring to detect active intrusion, and having robust response procedures and tools to limit the impact of an electromagnetic attack.

For defence applications, this means protecting sensors, platforms and the C5ISRT infrastructure from unauthorized intrusion, designing architecture with resilience and redundancy at the forefront, and having rapid detection of threats for response. For infrastructure and civil applications, this means protecting installations and networks and having the appropriate response procedures against electromagnetic attack.

Calian Solutions for the Digital Battlefield

Anti-Jamming GNSS Antennas

Global navigation satellite system (GNSS) technology has become an integral part of our daily lives, powering everything from navigation apps on our smartphones to critical infrastructure in aviation, telecommunications and defence. But, as GNSS technology becomes prevalent, so does the presence of interference—both intentional jamming and congestion of electromagnetic signals—which can overpower weak GNSS signals. Interference either degrades accuracy or can lead to complete loss of signal. To improve signal reception for GNSS antennas, Calian developed anti-jamming technology that supports performance in a jammed environment.

Calian anti-jamming antennas combine innovative design with advanced filtering to address today's GNSS challenges.

Learn more

Counter-UAS Solutions

Secure installations and facilities can be observed more easily today than ever before with the proliferation of small, commercial uninhabited aerial systems (UAS or drones). Hobby enthusiasts and kids alike can pilot small drones for fun, and they can also be used by malign actors to observe critical infrastructure like nuclear power plants, electricity infrastructure or military facilities. For smuggling, small drones are well suited to moving contraband across international borders or into controlled facilities like prisons. For civil aviation, keeping all UAS types away from airport flightpaths is essential for the safe and secure operation of airports. Calian provides a counter-UAS solution that detects unauthorized UAS flying into controlled airspace, identifies them as a threat, and then provides electronic defeat to force the UAS to the ground. Working alone or in sequence, at a stationary post or mobile on a vehicle, our C-UAS solution has a wide detection range for point defence, area defence, or a line defence along a border to keep unauthorized UAS out of places they shouldn't be.

Emissions Security & TEMPEST Devices

Calian delivers emissions security (EMSEC) solutions, recognized by the Canadian government and by TEMPEST standards. We protect facilities, infrastructure, networks and devices to safeguard sensitive data from electrical and electromagnetic threats. This starts with a harmonized threat risk assessment to identity where your facilities, infrastructure and equipment could be vulnerable to electronic intrusion. We deliver zoned assessment for any facility—government or industrial—that has zones with higher security requirements embedded in lower security facilities.

We tailor our emissions security solutions—including products—by modifying off-the-shelf equipment to meet your specific needs, all while meeting TEMPEST certification standards. We secure workstations, routers and switches, printers and scanners, ruggedized and non-ruggedized laptops and tables, and provide RF lockboxes.

Portfolio of Integrated Cyber Solutions

Following the NIST framework, Calian is your trusted partner in cybersecurity, offering a complete solution to protect your business. Calian enhances cybersecurity with 24×7×365 services, leveraging AI-driven threat detection, real-time monitoring and proactive protection against bad actors.

Whether your requirement is to manage an operations centre (SOC/NOC), detect and respond, assess vulnerabilities, or train your infrastructure teams for response readiness, the Calian cyber solutions team is there. Underpinned by Microsoft's world class next-gen Sentinel SIEM and Defender, organizations can monitor, detect and respond across endpoints, identities and IoT properties.

Data Interoperability Solutions

Modern militaries deploy with a range of different systems within their C5ISRT architecture. Electromagnetic attacks typically focus on individual sensors or systems operating on a particular frequency to maximize the impact and likelihood of a successful attack. By taking a systems-agnostic approach to interoperability, Calian delivers a "plug-and-play" approach through our virtual command and control interface (VCCI). This means active monitoring of data flows in and out and providing a customized approach to match the threat environment.

Our audio distribution service (ADS) allows us to connect voice and tactical data networks and conduct concurrent data capture. This approach also allows network managers to reconfigure networks to operate on different frequencies to evade jamming or intrusion. This provides protection through flexibility and agility, adapting to electromagnetic activities.

Customers and Sectors

Defence & National Security

We provide data sovereign solutions for defence and national security customers in Canada to protect installations, infrastructure and networks. They trust us when they cannot fail.

Space

The ground station is the most vulnerable part of the space ecosystem. Our solutions protect physical infrastructure on the ground to keep satellites on-time and on-target.

Health

Our Canadian healthcare industry is a complex, multi-layered environment, but appetizing to bad actors. Calian is known within healthcare as the go-to cyber and cloud modernization solutions company that can be counted on 24×7×365 to protect individual healthcare IP.

Transportation

Calian supports this critical infrastructure every day. Managing security and network operational environments, cloud management backup and redundancy, and RF emissions control enables airports to operate and service civilian demands with minimal risk.

Our Certifications

Calian SOC and IR Teams' Certifications

- Certified Threat Intelligence Analyst (CTIA)
- Certified Digital Forensics Examiner (CDFE)
- Certified Incident Handler (GCIH)
- Certified Information Systems Security Professional (CISSP)

Microsoft Certifications

- Microsoft Security, Compliance and Identity Fundamentals (SC-900)
- Microsoft Azure Fundamentals (AZ900)
- Microsoft Security Architects Expert (SC100)
- Microsoft Security Operations Analyst (SC200)
- Microsoft Identity and Access Administrator (SC300)
- Microsoft Information Protection Administrator (SC400)
- Microsoft Azure Security Engineer Associate (AZ500)

References

1. Matthew Slusher, 'Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information and Resilience,' Centre for Strategic & International Studies. 2 May 2025. Link ▶
2. The Economist, 'Fighting the war in Ukraine on electromagnetic spectrum,' 5 February 2025. Link ▶
3. Thoman Nilsen, 'Russian jamming is now messing up GPS signals for Norwegian aviation practically every day,' Barents Observer. 26 February 2024. Link▶
4. Johnathan, 'NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation,' The Record. 11 August 2023. Link ▶

CALIAN
Confidence. Engineered.

For over 40 years, Calian has delivered mission-critical solutions when failure is not an option. Trusted worldwide, we empower organizations in critical industries to overcome obstacles, manage risks and drive progress. By combining the expertise of our people, proven industry insight, cutting-edge technology, bold innovation and global reach, we deliver tailored solutions that solve complex challenges. Headquartered in Ottawa, Canada, with over 5,000 people around the world, Calian's solutions protect lives, strengthen security, foster global connectivity and drive economic progress, making a lasting impact where and when it matters most.

calian.com | info@calian.com | 1.877.225.4264 |