Brochure

XEdge for Cybersecurity and the Military

Cybersecurity Analysis, Constant Monitoring, and Military Labs in 5G Environments

XEdge is a Linux-based user equipment (UE) probe with support for up to four SIM cards, band-locking for frequency-specific analysis, and unattended remote operation.

While not a firewall or IDS, XEdge provides ground-truth intelligence on how networks behave under cyber or electronic attack.

About XEdge

- It validates resilience across operators, frequency bands, and applications, and can host third-party security agents for extended use in labs and live military environments
- It is ruggedized and vibration compliant, operates from -20°C to +55°C and can be deployed in forward operating bases, labs, or urban environments
- Its controller integrates via API into SIEM, SOAR, and C4ISR systems, turning raw performance data into actionable cybersecurity insight

XEDGE FOR CYBERSECURITY

1. Detecting and Validating Attack Impact

- **Jamming and RF Interference:** Continuous monitoring of throughput, latency, and SNR under jamming. In field exercises, confirms anti-jamming strategies; in labs, validates robustness of military 5G deployments
- **Spoofing and Rogue Base Stations:** Detects IMSI catchers or fake gNodeBs by flagging unexpected PLMN IDs, encryption downgrades, or forced frequency shifts
- **Overload and DDoS Simulation:** Generates high traffic loads (up to 6 Gbps aggregate) to simulate DDoS and measure resilience of mission-critical apps (AR goggles, drone feeds)

2. Anomaly and Alerting Capabilities

- **Real-Time Alerts:** Automated thresholds highlight unusual error spikes, jitter, or call drops
- **Baseline vs Deviation:** Establishes secure-performance baseline (latency, jitter, handovers) and flags drift caused by misconfigurations or cyberattack
- **Cross-Band Analysis:** Locks to bands (e.g., n78 mid-band vs baseline) for side-by-side comparison of resilience under interference or spoofing

3. Multi-Network and Multi-SIM Assurance

- **Four SIMs in Parallel:** Monitors up to four operators at once. If one network degrades under attack, others act as a control baseline
- **Failover Validation:** Confirms whether backup networks maintain QoS in live operations
- **Benchmarking Configurations:** Compare private 5G slices with strict encryption against public 5G for performance impact

Cyber Threat	XEdge Role	Outcome
Jamming/Interference	Monitors RF KPIs under stress	Proof of resilience/alerts
Spoofing/Fake Cell	Detects rogue PLMN ID and band shifts	Attack validation and logging
DDoS / Overload	Generates controlled traffc floods	Service degradation analysis

4. Cybersecurity Lab and Red Team Testbed

- **Safe Attack Simulation:** Acts as victim UE in cyber ranges; records KPIs under MITM, jamming, or spoofing
- **Repeatable Metrics:** Time-stamped logs provide repeatable benchmarks for training, drills, and procurement tests

5. Hosting Security Agents and Forensics

- **Linux Host Environment:** Deploy IDS/IPS agents, packet capture, or honeypots directly. Scripts and updates managed remotely
- **Integration via API:** Feeds KPIs to SIEM, SOAR, or C4ISR systems for full situational awareness
- **Black Box Recorder:** Stores logs, packet traces, and KPIs for forensic analysis post-incident

6. Military Deployment Scenarios

- **Four SIMs in Parallel:** Monitors up to four operators at once. If one network degrades under attack, others act as a control baseline
- **Failover Validation:** Confirms whether backup networks maintain QoS in live operations
- **Benchmarking Configurations:** Compare private 5G slices with strict encryption against public 5G for performance impact

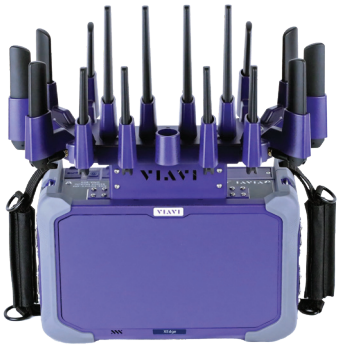
Key Value:

XEdge delivers ground-truth network intelligence under cyber stress. It detects spoofing, jamming, and overloads; validates resilience across bands and operators; and integrates with military cybersecurity frameworks for both real-time operations and forensic investigation.

XEDGE FOR THE MILITARY

XEdge for Military Private 5G Networks

- Multi-carrier, RF probe sensor-based, edge monitoring solution for continuous network testing and analysis
- Empower connectivity across every mobile network environment with the premier solution for edge network intelligence and SLA monitoring leveraging cloud-based remote access, AI analytics, and integration into operation.



	Application	Benefit
Ensuring Network Reliability	Deploy XEdge probes at fixed installations and mobile units to continuously monitor 5G network performance.	Real-time alerts for outages ensure uninterrupted communication for mission-critical operations.
Optimizing Coverage	Conduct walk tests inside buildings and drive tests across expansive bases to map 5G coverage and identify weak spots.	Heat maps and geo-fencing analytics allow repositioning antennas or deploying additional small cells
Stress Testing	Use XEdge as a traffic generator to simulate high-bandwidth scenarios from multiple units.	Validates the network's capacity to handle peak loads during intense operations like coordinated assaults
Rapid Deployment Support	Leverage unattended operation and remote management to monitor newly deployed 5G networks in field locations.	Reduces the need for on-site RF engineers, allowing rapid setup with minimal personnel.
Iot and Edge Computing	Integrate XEdge with military IoT ecosystems to monitor latency and bandwidth on the 5G network.	Ensures low-latency connections for edge applications like real-time threat detection or automated logistics.
Compliance, Reporting and Security	Leverage automated compliance reporting, historical data storage, and XEdge's RF monitoring with edge intelligence to document network performance and detect unauthorized mobile signals or jamming attempts in restricted zones.	Provides auditable proof of network reliability for post-mission reviews or infrastructure investments, with automated alerts for security teams and historical data to identify interference patterns.

SELLING THE SOLUTION

Persona: Military Communications/ Spectrum Operations Officer

- Role description: Plans, deploys, and assures secure private-5G/tactical-cellular communications across fixed bases, vehicles, and forward operating positions.
- Accountable for mission-critical uptime, spectrum compliance, and cyber-hardening while working with lean RF resources.

Pain Points	1. Maintaining reliable coverage for troops, sensors, and C2 links across rugged terrain and mobile units. 2. Need to stand-up and validate secure 5G networks at new forward operating bases (FOBs) within hours, not days. 3. Ensuring encryption and network security across all tactical links without manual, error-prone checks.
Motivators	1. Guarantee uninterrupted command-and-control to safeguard lives and mission success. 2. Gain "single-pane" visibility across private 5G, public LTE/5G, and WiFi to speed incident response. 3. Automate testing and alerting to conserve scarce RF personnel and budgets.
Discovery Questions for this Persona	1. When you deploy a new FOB or convoy, how do you currently validate 5G coverage and performance? 2. What is your mean time to detect and isolate a network issue during live exercises? 3. Which systems need live network KPIs ingested into your situational-awareness dashboards?
Ways that XEdge Addresses the Persona's Needs or Pain	1. Quad-radio, multi-operator probes — simultaneously monitor private 5G, public carriers, and MVNO profiles. 2. Automated drive and walk tests — geo-fenced routes and remote triggers slash truck-rolls while producing heat-maps of coverage around critical assets.

XEdge — the premier solution for edge network intelligence and SLA monitoring leveraging cloud-based remote access, AI analytics, and integration into operation.

viavisolutions.com

Contact Us +1 844 GO VIAVI | (+1 844 468 4284)
To reach the VIAVI office nearest you, visit viavisolutions.com/contact
sales.xedge@viavisolutions.com

xedge-cybersecurity-military-br-maa-nse-ae
30194591 900 0925