

# Leveraging Strategic and Actionable Paths in Cybersecurity and Resilience to Safeguard the Black Sea Region.

## Executive Summary

The Black Sea has become one of the most contested operational theaters in the world. Cyber operations, electronic warfare, and conventional military activity now intersect across maritime, energy, logistics, and communications networks. What was once sporadic disruption has become the daily baseline. Navigation interference, degraded communications, and attacks on operational technology at ports and power stations are no longer unusual events but persistent realities.

Resilience cannot depend on years of debate or delayed consensus. Governments, operators, and industry must take practical steps now to harden critical nodes, ensure continuity of operations under degraded conditions, and expand Europe's defense industrial base so interoperable solutions can be fielded quickly and at scale. This paper examines the current threats, outlines the resilience measures that can be implemented most effectively, and describes how both large primes and small and medium-sized enterprises (SMEs) can contribute to building capacity.

## Shifts in the Threat Environment

The operational landscape in the Black Sea has undergone significant changes. Navigation and spectrum interference, particularly the jamming and spoofing of Global Navigation Satellite Systems (GNSS), has moved from being an occasional disruption to a constant feature of the region. Pilots and ship operators increasingly assume degraded signals as a matter of course. This is not an abstract risk because a misrouted unmanned aerial vehicle (UAV) or commercial vessel can quickly escalate into a cross-border incident.

Communications are equally vulnerable. Both satellite and terrestrial links have been repeatedly targeted, exposing a dangerous dependence on single providers and leaving critical command-and-control systems, UAV operations, and logistics networks vulnerable to disruption. At the same time, adversaries are focusing more heavily on operational technology (OT), which includes the industrial systems that control physical infrastructure. Malware targeting port cranes in Constanța, fueling systems at forward bases, and substations along regional energy grids demonstrates that attackers are actively seeking to disrupt the essential services that underpin mobility and power.

Persistent vulnerabilities in the supply chain compound these threats. Incomplete Software Bills of Materials (SBOMs), opaque update processes, and limited local repair capacity leave nations dependent on vendors that may not be able to respond quickly during a crisis. Taken together, these developments mean operators can no longer plan on the assumption of reliable navigation and communications. The new baseline includes contested positioning, navigation, and timing (PNT), intermittent connectivity, and supply chains that are vulnerable to compromise.



### **The Paths to Strategic and Actionable Resilience**

Responding to this environment requires a shift in both mindset and practice. Positioning, navigation, and timing (the core functions that enable aircraft, ships, and networks to operate with precision) must be reinforced with multi-constellation GNSS, anti-jam antennas, and inertial or radar backups that do not depend on satellite signals. Interference monitoring should be prioritized at key ports and airbases, and leaders should regularly assess how long critical missions can be sustained without external satellite inputs.

Communications should be managed as a cohesive portfolio, not as separate channels. Satellite, terrestrial, and high-frequency (HF) radio links need to be coordinated with tested failover procedures and clear protocols for maintaining priority services. Commanders and operators must trust that switching between channels under pressure will function reliably.

Operational technology needs segmentation and security enhancements. Safety systems, such as those controlling fuel distribution or crane operations, should be isolated from business networks managing administrative data. One-way gateways that permit data to flow outward but block incoming traffic should become standard practice. Up-to-date SBOMs should be maintained for critical assets to identify and fix vulnerabilities quickly. Manual reversion procedures (fallback methods allowing equipment operation without automation) should be rehearsed to ensure essential functions can continue if digital controls fail.

Regional cooperation is also essential. A notification compact for navigation and communications anomalies, complete with agreed severity scales and designated points of contact, would replace the current reliance on informal channels with a predictable framework. Such arrangements reduce confusion in crises and help maintain coordination across borders.

Finally, supply chain integrity must be reinforced. Vendors should be required to deliver SBOMs and transparent vulnerability management processes, while governments and industry partners should invest in developing local repair and manufacturing capacity. For systems expected to operate into the 2030s, planning for post-quantum cryptography (a new generation of encryption designed to resist quantum computing) should start now to prevent expensive retrofits later.

### **Mobilizing Industry at Scale**

Industry will respond most effectively when governments clearly outline operational requirements. Instead of vague calls for better cybersecurity, procurement should target measurable results, such as keeping port operations running for seventy-two hours during contested navigation and intermittent communications. These specific requirements enable vendors to provide integrated and interoperable solutions rather than isolated tools.



Standardizing reference architectures and interfaces is just as important. When ports, bases, and energy grids follow common designs, suppliers can offer solutions with less customization, which cuts costs and delays. Coalition labs and cyber ranges should be used not only for training but also for pre-award validation, making sure proposed systems can operate during GNSS denial, work well with mission networks, and stay safe in OT environments. This method also helps reduce barriers for SMEs, which often offer innovative technologies but lack the resources for custom integration.

Onramps already exist for smaller firms through NATO's Defence Innovation Accelerator for the North Atlantic (DIANA), the NATO Innovation Fund, the NATO Communications and Information Agency (NCIA) procurement frameworks, and EU programs such as the European Defence Fund. These mechanisms enable modular technologies like sensors, analytics tools, and data gateways to be integrated into larger prime-led solutions. Building a stronger pipeline of OT-literate cyber technicians will be equally important to ensure that technical capacity keeps pace with procurement.

### **Measuring Progress**

Resilience should be monitored using readiness-based metrics rather than compliance checklists. Leaders need to understand how many hours critical missions can operate without GNSS, how quickly systems can return to minimum operations after a mixed IT and OT incident, and whether failover procedures are effective under real stress conditions. The proportion of OT assets in segmented zones with current SBOMs, the frequency of patching cycles, and measurable improvements in detection and response times across drills all serve as important signs of progress.

### **Call to Action**

The Black Sea will remain a testing ground for hybrid conflict. Effective defense here is not about stopping every intrusion but about keeping operations running and preventing adversaries from achieving their goals through disruption. Practical steps are already available. Strengthening navigation and timing systems, diversifying communications, segmenting operational technology, improving information sharing, and building more resilient supply chains can all be implemented today. Taken together, these measures will reduce vulnerabilities, strengthen Europe's defense industrial base, and boost regional resilience. The challenge is not whether solutions exist but whether governments and industry will act quickly enough to deploy them.

### **About Us**

Venatôre LLC delivers secure, integrated, and mission-ready technology solutions to U.S. Defense, Intelligence, and Civilian agencies. It provides support in the areas of [Cyber Resiliency](#), [Digital Infrastructure](#), [Data Dominance](#), [Supply Chain Management](#), and [Software-Defined Advantage](#). When speed, clarity, and security matter, Venatôre executes with confidence. To learn more, visit our website [www.venatore.com](http://www.venatore.com). Follow us through our corporate page on [LinkedIn](#).