VALCORE DEFENCE // C-SUITE COMPLIANCE & RESILIENCE

NIS2 & CER: C-SUITE ACCOUNTABILITY

Operational Resilience in the Era of Converged Cyber-Physical Threats — Audience: C-Suite, Boards & Family Offices

EXECUTIVE SUMMARY

The regulatory landscape for corporate security in Europe has undergone a seismic shift. The introduction of the **NIS2 (Network and Information Security)** and **CER (Critical Entities Resilience)** directives ends the era of treating security as a purely operational IT or facility management issue. Today, security is a direct legal liability for the Board of Directors.

1. NIS2: THE NEW ERA OF PERSONAL LIABILITY

The NIS2 Directive forces organizations to adopt a proactive, all-encompassing approach to cybersecurity. The most critical and disruptive shift is the introduction of Executive Accountability:

- **Personal Liability (Article 20):** Management bodies (C-Suite, Board of Directors) must formally approve cybersecurity risk-management measures and actively oversee their implementation. If a breach occurs due to negligence or lack of systemic oversight, executives can be held personally liable and temporarily suspended from their managerial functions.
- **Supply Chain Vulnerability:** Organizations are now legally responsible for the security of their entire supply chain. A breach at a third-party vendor (e.g., an unprotected logistics provider, unvetted contractor, or travel management company) represents a direct compliance failure for the primary entity.
- **Severe Financial Penalties:** Non-compliance can result in fines up to €10 million or 2% of total worldwide annual turnover, whichever is higher, making non-compliance a direct threat to corporate survival.

2. CER: PHYSICAL RESILIENCE & SABOTAGE

While NIS2 handles the digital realm, the CER Directive mandates the protection of physical infrastructure and operations against natural hazards, terrorism, and sabotage. The European Union explicitly recognizes that **Cyber-Physical Convergence** is the modern threat reality:

- **Comprehensive Risk Assessments:** Entities must conduct continuous, rigorous risk assessments mapping both physical and operational vulnerabilities, including supply chain routes, facility perimeters, and executive travel exposure.
- **Mandatory Background Checks:** Enhanced vetting (Due Diligence and OSINT) is legally required for personnel holding sensitive roles or having access to critical infrastructure, sensitive data, and executive itineraries.

- **Incident Response Timelines:** Strict reporting obligations mandate that significant physical or cyber-physical incidents must be reported to national authorities within hours, requiring an always-on, proactive intelligence monitoring system.

3. THE CONVERGENCE MANDATE

The core message of both directives is unified: siloed security fails. A cyberattack often precedes a physical breach (OSINT gathering, system hijacking), and physical access is frequently used to execute a cyberattack (rogue devices, insider threats). Meeting the rigorous requirements of NIS2 and CER demands a holistic risk management framework—combining **VALCORE DEFENCE C4ISR**, **Guardian Apex™ 100% Offline Edge AI**, and **SRD Rapid-Response Protection**.

IS YOUR BOARD OF DIRECTORS PREPARED FOR PERSONAL LIABILITY?
Compliance requires a proactive, converged protective intelligence architecture. To implement these systems, secure your operations, and protect your leadership from legal exposure, initiate secure contact with VALCORE DEFENCE Command.

VALCORE DEFENCE (Formerly Northstar Mobility) — Covert Executive Protection, Edge AI & C4ISR
🌐 https://valcore-defence.com | ✉️ operations@northstar-mobility.com