

Sustainability via Resilience: A Security Paradigm for Critical Infrastructure and Military Systems

The evolution of the threat landscape makes the transition from defensive security to adaptive, resilience-based security unavoidable. Resilience is no longer an optional feature but the primary metric of system effectiveness.

Systemic standards provide the structural foundation for this transformation, enabling modularity, interoperability, and strategic autonomy. In both civilian and military domains, the ability to continue operating under adverse conditions, rather than preventing all failures, defines true security.

By Dr. Gustavo Scotti di Uccio – AOS PGD¹

Executive Summary

The security of critical infrastructure and military systems is undergoing a structural transformation. Traditional approaches based on prevention and perimeter defence are no longer sufficient in the face of an increasingly complex threat environment characterised by adaptive adversaries, hybrid operations, and the pervasive use of artificial intelligence. In this context, resilience, defined as the ability to anticipate, absorb, adapt, and rapidly recover from disruption, has emerged as the primary indicator of system effectiveness.

Recent analyses by the European Union Agency for Cybersecurity and the National Cyber Security Centre confirm a significant increase in large-scale, multi-vector cyberattacks targeting essential services and national security assets. These attacks are no longer isolated incidents but components of coordinated campaigns that combine cyber, physical, and informational dimensions.

At the same time, threat actors, both criminal and state-sponsored, have evolved into resilient ecosystems. According to Europol, these actors operate through decentralised, modular, and redundant structures that enable rapid recovery and adaptation. This asymmetry places traditional, static defence models at a structural disadvantage.

The policy implication is clear: security can no longer be defined solely in terms of protection; it must be understood as the capacity to ensure continuity of operations under adverse conditions. This requires a transition towards resilience-by-design, where systems are engineered to function even when partially compromised. The concept of controlled degradation, maintaining essential services at reduced capacity rather than experiencing total failure, is particularly relevant for both civilian and military domains.

Systemic standards are a critical enabler of this transition. By promoting interoperability and modularity, they allow systems to be reconfigured dynamically, components to be replaced rapidly, and dependencies to be managed more effectively.

A central dimension of resilience is technological sovereignty. Dependence on external suppliers, opaque technologies, or concentrated supply chains introduces systemic vulnerabilities that may be exploited in times of crisis or geopolitical tension. Open standards and modular architectures mitigate these risks by ensuring that systems remain accessible, adaptable, and controllable over time. In this sense, resilience and sovereignty are mutually reinforcing objectives.

For policy makers, the transition to a resilience-oriented paradigm requires coordinated action across governance, investment, and regulation. In the civilian domain, priority should be given to the modernisation of critical infrastructure through distributed architectures, enhanced cyber-physical integration, and robust incident response capabilities. Supply chain security and cross-sector information sharing must be strengthened to address systemic risks.

¹ AOS is an Independent company registered in Belgium since 2012. It delivers technical, engineering, operational and management support for defence and security sector at national, European & transatlantic levels. In systems engineering & programme management for the development of complex & innovative projects. In last 5 years, AOS has carried out more than 80 NATO studies and EU projects in interoperability, emerging technologies, air defence, energy management, UAVs, & dual-use solutions. AOS team consists of senior managers & engineers from Belgium, the Cz. Rep., France, Germany, Italy, Luxembourg, Portugal & Spain with extensive experience in defence industries, Ministries of Defence, and EU institutions

In the defence domain, resilience must be embedded as a core operational requirement. Military systems should be designed to sustain mission effectiveness under contested conditions, leveraging modular open system approaches, distributed command-and-control structures, and advanced data architectures. Integration across cyber, electronic, and kinetic domains is essential to ensure operational continuity in multi-domain environments.

Ultimately, resilience represents a shift from a reactive to a strategic posture. It enables states and organisations not only to withstand disruption but also to maintain strategic coherence and operational effectiveness in uncertain and hostile environments. As the threat landscape continues to evolve, the ability to adapt and continue operating under pressure will define both security and competitiveness.

Failure to adopt this paradigm risks not only increased vulnerability but also loss of strategic autonomy. Conversely, timely investment in resilience and systemic standards offers a pathway to sustainable security, economic stability, and credible defence capability.



The security environment surrounding critical infrastructure and military systems has undergone a significant transformation over the past decade. The convergence of cyber, physical, and informational domains has resulted in increasingly complex and interdependent risk scenarios. Attacks are no longer isolated events but components of broader, coordinated campaigns that can produce cascading effects across sectors and national boundaries.

Recent incidents illustrate how vulnerabilities can rapidly translate into strategic disruptions. These cases demonstrate that the traditional security paradigm is insufficient to address contemporary threats.

In response, resilience has emerged as a central concept in both policy and operational contexts. Rather than attempting to eliminate all risks, resilience-based approaches assume that disruptions are inevitable and focus on ensuring

continuity of operations under adverse conditions. This paper investigates this paradigm shift and its implications for system design, governance, and strategic autonomy: resilience as a systemic property, integrating four core dimensions: robustness, adaptability, recoverability, and transformability.^{2,3}

Recent data across Europe confirm this trend. According to the European Union Agency for Cybersecurity⁴, the cyber threat landscape has become significantly more complex, with a marked increase in large-scale, multi-vector attacks targeting essential services. Similarly, the National Cyber Security Centre⁵ has reported a steady rise in nationally significant incidents affecting both public and private sectors, particularly in areas linked to national security and defence. These developments indicate not only a quantitative growth in attacks, but also a qualitative shift towards more adaptive and persistent threat models.

A notable example is the Colonial Pipeline ransomware attack⁶ in 2022, which disrupted fuel distribution across the United States, demonstrating

Security must shift from prevention to continuity: the ability to operate under attack is now more critical than the ability to prevent breaches.

how cyber incidents can rapidly escalate into physical and societal crises. In Europe, cyberattacks against hospitals during the COVID-

² E. Hollnagel, *Resilience Engineering in Practice*, Ashgate, 2011.

³ D. Woods, "Four concepts for resilience and the implications for the future of resilience engineering," *Reliability Engineering & System Safety*, vol. 141, pp. 5–9, 2015.

⁴ ENISA Threat Landscape reports: <https://www.enisa.europa.eu/publications>

⁵ NCSC Annual Review: <https://www.ncsc.gov.uk/section/about-ncsc/annual-review>

⁶ US Dep of Energy: https://cyote.inl.gov/content/uploads/24/2025/12/CyOTE-Case-Study_Colonial-Pipeline.pdf

19 pandemic further illustrated the vulnerability of critical services under stress conditions.

Within this context, the limitations of traditional security strategies become increasingly evident. Static protection measures are no longer sufficient against threats that evolve in real time. Despite growing investments in security across Europe and the United Kingdom, organisations continue to experience prolonged service disruptions following successful attacks. The critical issue is no longer whether a breach will occur, but whether systems can continue to operate and recover swiftly under adverse conditions.

This challenge is particularly acute in the domains of critical infrastructure and military systems, where operational continuity is a strategic requirement. Recent incidents have demonstrated that sectors such as energy, healthcare, transport, and advanced manufacturing can be disrupted with consequences that extend far beyond the digital domain, affecting physical security and societal stability. In military contexts, even temporary degradation of operational capability can provide a decisive advantage to adversaries.

Ransomware provides a clear illustration of this evolution. According to joint assessments and threat reports from the European Union Agency for Cybersecurity⁷ and the National Cyber Security Centre⁸, ransomware attacks have shifted from system disruption towards data exfiltration and strategic coercion. Increasingly, the objective is not merely to deny access, but to extract sensitive information and exert operational or psychological pressure. Organisations equipped with resilient architectures, featuring redundancy, segmentation, and rapid isolation capabilities, are able to maintain essential functions and limit damage. In contrast, monolithic systems tend to fail catastrophically, with recovery times incompatible with operational requirements.

Cybercrime has evolved into a structured, adaptive ecosystem. According to Europol, criminal networks exhibit characteristics typical of resilient systems: decentralisation, modularity, and redundancy. When disrupted, they rapidly reconfigure, reusing infrastructure and expertise, a phenomenon often referred to as the “hydra effect.”

State-sponsored actors operate similarly, leveraging distributed command-and-control architectures, AI-assisted reconnaissance, and multi-domain operations. For instance, cyber operations observed during the Russian invasion of Ukraine combined cyberattacks on energy infrastructure with electronic warfare and kinetic

strikes, demonstrating the convergence of digital and physical domains. These developments highlight a key point: adversaries already operate according to systemic resilience principles. Defensive systems that remain static and perimeter-focused are structurally disadvantaged.

A particularly relevant observation is that adversaries themselves provide an implicit model for resilience.

Contemporary cybercriminal and state-sponsored networks are decentralised, distributed, and highly adaptive,

Adversaries already operate as resilient systems; defending static infrastructures against dynamic ecosystems creates a structural asymmetry.

as documented by Europol. Their effectiveness does not depend on protecting individual components, but on the resilience of the overall ecosystem. This suggests that resilience cannot be treated as an add-on feature; it must be embedded within system architecture from the outset.

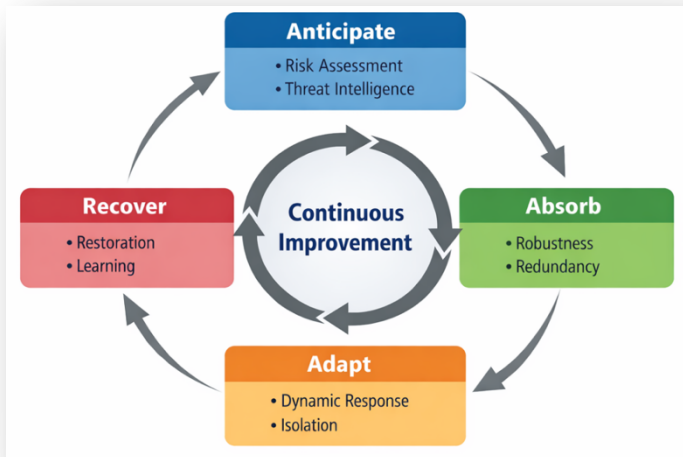
In this scenario, systemic standards play a pivotal role. They go beyond technical specifications, enabling the creation of interoperable, modular, and governable ecosystems. The adoption of shared standards allows compromised components to be replaced rapidly, facilitates the integration of heterogeneous solutions, and ensures continued control over critical technologies even during crises. Moreover, such standards enhance transparency and auditability, which are essential in high-assurance environments such as defence.

The link between systemic standards and technological sovereignty is direct. Sovereignty is not limited to ownership of technology; it encompasses the ability to understand, modify, and sustain it over time. At the European level, this perspective is reflected in strategic initiatives promoted by the European Commission, aimed at strengthening digital autonomy and securing critical supply chains. In the United Kingdom, similar principles underpin national cybersecurity strategies coordinated by the National Cyber Security Centre. In an increasingly unstable geopolitical environment, dependence on external suppliers or opaque proprietary solutions represents a significant risk. Open standards and modular architectures mitigate this risk by ensuring operational continuity even in the event of supply chain disruption or political constraints.

⁷ EU Cybersecurity Strategy: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

⁸ UK Cyber Security Strategy: <https://www.ncsc.gov.uk/collection/national-cyber-security-strategy>

Adopting a resilience-oriented approach yields tangible and measurable benefits. Operational continuity can be maintained even under attack, significantly reducing downtime. The economic impact of incidents is mitigated through faster recovery and more effective containment. Systems become inherently more adaptive, capable of evolving alongside emerging threats without requiring fundamental redesign. At the same time,



strategic autonomy is reinforced, a critical factor for both civilian infrastructure and military capability.

This transformation also entails a fundamental shift in the security paradigm. The objective is no longer to build ever-higher defensive barriers, but to design systems capable of functioning even when those barriers are breached.

Within this evolving context, resilience emerges as a fundamental design principle. Rather than focusing exclusively on preventing intrusions, resilient systems are conceived to absorb shocks, adapt dynamically, and recover rapidly while maintaining essential operations. This perspective introduces the notion of controlled degradation, whereby systems continue to function, albeit at reduced capacity, instead of experiencing total collapse. Such an approach is particularly critical in sectors where operational continuity is directly linked to societal stability or strategic advantage.

The SolarWinds supply chain attack⁹ is a paradigmatic case: attackers infiltrated trusted software updates, compromising thousands of

organisations globally, including government agencies and defence contractors.

These events demonstrate that breaches are no longer exceptional occurrences but should be considered inevitable

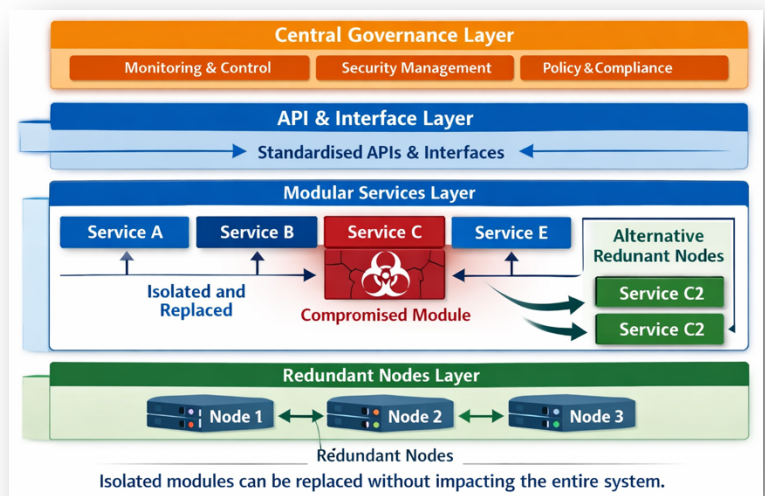
Resilience is not a feature but a systemic property that must be embedded at the architectural level.

within complex, interconnected systems. Consequently, the central question shifts from whether a compromise will occur to whether systems are capable of maintaining functionality and recovering efficiently under adverse conditions.

Traditional cybersecurity strategies, based on firewalls, intrusion detection, and access control, assume that threats can be prevented or contained at the boundary. However, modern attack vectors such as supply chain compromise, zero-day vulnerabilities, and insider threats bypass these controls.

The key question is no longer *if* systems will be compromised, but *how well they can absorb, adapt, and recover from disruption*.

The evolution of the threat landscape makes the transition from defensive security to adaptive security unavoidable. Resilience emerges as the primary indicator of system effectiveness, while systemic standards provide the enabling framework. For critical infrastructure and military systems, this requires a fundamental rethinking of



9

<https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack>

architectures, processes, and governance models, embracing an approach in which the capacity to adapt and continue operating is not optional, but essential. The adoption of widely recognised frameworks, including ISO/IEC 27001 for information security management, ISO 22301 for business continuity, and the NIST Cybersecurity Framework¹⁰, supports the implementation of consistent and verifiable resilience practices. At the European level, initiatives promoted by the European Commission aim to harmonise cybersecurity policies and strengthen digital sovereignty, particularly through regulatory instruments such as the NIS2 Directive. These efforts reflect an increasing awareness that resilience is not solely a technical issue but also a matter of governance and strategic coordination.

The relationship between systemic standards and technological sovereignty is particularly significant. Sovereignty, in this context, extends beyond ownership of technological assets to encompass the ability to understand, modify, and sustain them over time. Dependence on external suppliers or opaque proprietary solutions introduces vulnerabilities that may be exploited during geopolitical crises or supply chain disruptions. Open standards and modular architectures mitigate these risks by ensuring that systems remain controllable and adaptable, even in the face of external constraints.

From an operational perspective, the adoption of a resilience-oriented approach yields measurable benefits. Systems designed according to resilience principles are capable of maintaining operational continuity under attack, thereby reducing downtime and mitigating economic and societal impacts. They are inherently more adaptive, enabling incremental evolution in response to emerging threats without requiring fundamental redesign. In addition, such systems contribute to reinforcing strategic autonomy, a critical objective for both civilian infrastructure and military capability in an increasingly uncertain geopolitical environment.

Resilience and technological sovereignty are mutually reinforcing: without control over systems, resilience cannot be guaranteed.

In the civilian domain, the implementation of resilience requires a comprehensive rethinking of critical

infrastructure design and management. This includes the adoption of distributed and modular

architectures, the integration of cyber and physical security measures, and the development of robust incident response and recovery capabilities. Particular attention must be paid to the protection of industrial control systems and the security of supply chains, which represent critical points of vulnerability.

Moreover, the promotion of interoperability and information sharing among stakeholders is essential to ensure coordinated responses to large-scale disruptions.

In defence, resilience is not only a technical requirement but an operational capability.

In the military domain, resilience assumes an even more strategic dimension. Systems must be designed to support mission continuity under contested conditions, including cyberattacks, electronic warfare, and physical disruption. This entails the adoption of modular open system approaches, distributed command-and-control structures, and autonomous fallback capabilities. The integration of cyber intelligence into operational planning and the use of artificial intelligence for anomaly detection further enhance situational awareness and decision-making. Continuous testing through exercises and simulations is also essential to ensure that systems and personnel are prepared to operate in degraded or denied environments.

In conclusion, the transformation of the threat landscape renders the transition from defensive to adaptive security paradigms unavoidable. Resilience emerges as the primary indicator of system effectiveness, while systemic standards provide the enabling framework for its implementation. For both critical infrastructure and military systems, this implies a fundamental reconfiguration of architectures, processes, and governance models. In such a context, the capacity to adapt, absorb disruption, and continue operating under adverse conditions is no longer an optional attribute but a defining requirement of modern security.

¹⁰ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2022.