ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Supply Chain Security and AI Risk Governance Model for Critical Infrastructure under NIS2, CER, and CRA

Natalija Parlov | Apicura Cert, University of Zadar, Croatia | ORCID: 0000-0002-8468-7465

Gordan Akrap | Military Leadership and Management, Dr. Franjo Tuđman Defense and Security University, Croatia | ORCID: 0000-0003-2666-596X

Josip Esterhajer | Military Leadership and Management, Dr. Franjo Tuđman Defense and Security University, Croatia | ORCID: 0009-0000-7215-1228

Abstract

Critical infrastructure increasingly depends on digital ecosystems where external providers, artificial intelligence (AI)-based tools, and complex supply chains form the backbone of essential services. This interconnectedness generates cascading risks that surpass the scope of internal controls, exposing sectors, such as energy, water, food, healthcare, and transport to systemic vulnerabilities. Known incidents illustrate that supply chain compromise is not a theoretical possibility but persistent and growing reality. According to the authors' practical experience in national security and sectoral information security, cybersecurity and resilience-oriented projects, organisations often struggle to recognise context of the threats in their critical services, wideness, and vulnerabilities of own supply chain and/or translate standards and new regulatory requirements into daily operational measures, which is a gap this model seeks to address. The purpose of this paper is to underline why supply chain and AI-related risks represent a systemic challenge for critical infrastructure, demonstrate how

Received: 8.06.2025

Accepted: 8.10.2025

Published: 05.12.2025

Cite this article as:
N. Parlov, G. Akrap, J. Esterhajer, "Supply chain security and AI risk governance model for critical infrastructure under NIS2, CER, and CRA," ACIG, vol. 4, no. 1, 2025, doi: 10.60097/ACIG/211823

Corresponding author:
Natalija Parlov, APICURA CERT, University of Zadar, Zagreb, Croatia; E-mail: una@apicura.hr
0000-0002-8468-7465

existing standards and regulatory frameworks can be synthesised into a coherent governance model and provide organisations with a practical tool that moves towards operational resilience. The chosen methodology rests on comparative analysis of chosen international standards (ISO 28000, ISO 31000, ISO/IEC 27001/27002/27005, ISO/IEC 23894, ISO/IEC 42001, and NIST AI RMF), supported by European Union obligations and recent European Union Agency for Cybersecurity [European Network and Information Security Agency] (ENISA) recommendations. Five-step supply chain security and AI risk governance model contribute structured, practical step-by-step model for strengthening systemic resilience. As an immediate step, operators should insert at least one supply chain-specific clause into their next procurement or renewal contract: a clear timeline and format for incident notification by the supplier.

Keywords

risk management, hybrid threats, supply chain security, artificial intelligence risks, critical infrastructure resilience

1. Introduction

Ensuring the security of supply chains in critical infrastructure is a strategic imperative, particularly under the regulatory framework of the Network and Information Systems 2 (NIS2), Critical Entities Resilience (CER) Directives [1, 2] and the Cyber Resilience Act (CRA) [3]. Organisations classified as essential or important entities must manage not only internal cyber resilience but also the growing risks posed by third-party suppliers and service providers.

Resilience of critical infrastructure depends on far more than the strength of its internal systems. From energy and water to healthcare and transport – these essential services rely on complex supply chains that include software vendors, hardware providers, cloud platforms and increasingly – artificial intelligence (AI). As these systems grow more interconnected, supply chain has quietly become one of the greatest sources of risk. If not yet the greatest one, in some time soon definitely.

High-profile incidents like SolarWinds [4] and NotPetya [5, 6] have shown how easily attackers can bypass strong internal defences by targeting weaker links in the supply chain. Once inside, the damage can be widespread, cascading across sectors and borders, and even though these incidents were dated from 2017 and 2020, the

situation today is not much different. According to the authors' experience and discussions with operators in practice, the way these events are portrayed in literature and media sometimes oversimplifies the problem, while the real weaknesses often lie in smaller, less visible suppliers and their everyday security lapses. In our recent engagements, the most common root cause behind third-party incidents was the absence of software bill of materials (SBOM)-backed updates and unclear incident notification clauses in supplier contracts. SBOM is like an ingredient list for software – it shows which parts and libraries are inside, so organisations can quickly check for risks or vulnerabilities.

Many organisations, despite now having robust cybersecurity policies – continue to depend on third parties with vastly different standards, practices, and levels of visibility. Even suppliers who don't appear critical on paper may hold access to sensitive systems, data or operational dependencies. Adding to this complexity is the rapid (and often insufficiently governed or supervised) adoption of AI technologies across infrastructure and supply chains. It undoubtedly delivers benefits (from predicting failures to enabling automation), yet, according to the authors' experience, the associated risks are often underestimated or misinterpreted. Literature and media frequently emphasise sensational scenarios – while in practice the more serious threats stem from accumulated data errors, unnoticed supply chain dependencies, or unclear contractual obligations with AI solution providers. Poorly governed AI systems can be manipulated, poisoned with malicious data, or even leveraged to scale and automate cyberattacks. More recent incidents, such as the MOVEit breach of 2023 [7], GhostAction GitHub supply chain campaign [8], and AI-specific threats like Model Namespace Reuse [9] illustrate that attacker sophistication and supply chain complexity continue to escalate.

In 2023/2024, the 3CX DesktopApp 'SmoothOperator' supply chain attack [10] exposed how a double compromise (via the software provider 3CX and a prior tampered application from Trading Technologies) can amplify damage, distributing trojanised installers signed with legitimate certificates. In March 2024, a critical backdoor was discovered in the widely used open-source XZ Utils compression library [11], demonstrating that even highly trusted components can be weaponised if governance is weak.

More recently, in 2025, a massive *npm* supply chain attack [12] pushed malicious updates to 18 popular JavaScript packages with more than 2 billion weekly downloads which was designed to

intercept cryptocurrency transactions. During the same year, third-party breaches impacted airlines: Air France/KLM [13] disclosed customer data exposure through vendor contact-centre platform, while Qantas [14] confirmed a compromise affecting up to 6 million customer records. At the same time, academic research throughout 2025 highlighted thousands of compromised packages in PyPI repositories and structural vulnerabilities across large language model (LLM) supply chains, revealing that both open-source ecosystems and AI models remain potent targets.

According to the authors' experience in working with critical infrastructure stakeholders, dependence on external providers, AI tools, and complex supply chains has become an operational reality. While this interconnectedness enables efficiency, in practice it often generates cascading risks that exceed the scope of internal controls and directly affect sectors such as energy, food, water, healthcare, and transport.

From a supply chain perspective, these cases confirm that vulnerabilities are rarely confined to a single organisation but they propagate through dependencies, open-source components, cloud platforms, and AI ecosystems – turning the supply chain itself into both the entry point for attackers and the amplifier of systemic disruption. In the context of critical infrastructure, such disruptions can quickly escalate into failures of essential services, undermining energy distribution, healthcare delivery, transportation safety, or even public administration. Unlike isolated corporate breaches, attacks on supply chain elements that feed into critical systems ripple outward, magnifying operational risks, eroding public trust, and exposing societies to cascading effects that extend well beyond the digital domain itself.

Artificial intelligence combines benefits with risks, often captured by the Dr. Jekyll and Mr. Hyde metaphor [15]: a technology that can function as trusted partner under control but transform into a dangerous liability when left unchecked. Without proper oversight, the same AI model that enhances decision-making and operational efficiency may silently undermine system integrity, misinterpret critical data, or be exploited for malicious purposes. What makes this particularly concerning is that many organisations rely on third-party AI tools or embedded models within supply chain solutions without full visibility into how these systems are trained, tested, or maintained. Or who else has the full and unrecognised/unreported access rights to them. As a result, they may unknowingly pose significant threat and inherit vulnerabilities they neither introduced nor can easily detect.

The problem lies not only in the data flows but also in the systemic factors that determine their security and resilience. Data leakage, unavailability, manipulation, misuse, or loss of integrity should be seen as outcomes, while the real problem often lies in the combination of internal and external threats and the absence of a strong security culture across organisations and their suppliers. Internal weaknesses, such as inadequate access controls, fragmented governance structures, poor incident reporting, or the lack of staff awareness create fertile ground for exploitation. External pressures, from targeted cyberattacks and ransomware campaigns to geopolitical tensions and hybrid operations, amplify these vulnerabilities and expose systemic fragility.

Security culture is equally important, yet often underestimated. Many organisations still treat resilience as a compliance task instead of an operational mindset. Without leadership commitment, cross-departmental collaboration, supplier alignment, adequate training programs, continuous awareness efforts and long-term investment in resilience – even the most sophisticated technical controls remain fragile. In this sense, technical failures are often only symptoms of deeper cultural shortcomings: insufficient prioritization of security at management level or a persistent gap between formal policies and everyday practices.

When these weaknesses converge the result can be severe: data may leak via insecure application programming interfaces (APIs), be encrypted by ransomware, manipulated through poisoned AI models, stolen via third parties, or destroyed by wiper attacks. These incidents are only the visible surface of the problem while beneath lies the challenge of aligning organisational culture, supplier governance, and national resilience strategies in a coherent and proactive way. Addressing data integrity is therefore not just about cybersecurity in a narrow sense but about strengthening systemic trust with operational continuity and public safety against both human error and deliberate exploitation.

Bearing this in mind, the European Union (EU) introduced the NIS2 Directive, CER Directive, and Cyber Resilience Act (CRA) which significantly raise the bar for how essential and important entities must approach threat recognition, risk management, supply chain oversight, and incident preparedness –areas that poses a clear signal that reactive security is no longer enough but that organisations must now take proactive, structured approach that spans the entire supply chain, including the AI systems and data flows. The key is always in the data – either in protecting it, accessing, or using it (with different motives).

To address these challenges – the purpose of this paper is not only to highlight the growing exposure of critical infrastructure to supply chain and AI-related risks but also to provide structured and auditable model that organisations can adopt. Methodology behind the model is grounded in a synthesis of chosen international standards and frameworks, chosen regulatory obligations (NIS2, CER, and CRA) and insights from the recent European Union Agency for Cybersecurity [European Network and Information Security Agency] (ENISA) reports. This approach was chosen deliberately: it ensures that the framework is compatible with existing management systems, aligned with EU compliance requirements, oriented towards organisational and technical measures to be taken and responsive to emerging AI-specific threats.

The primary goal is therefore two-fold: first to bridge the gap between compliance and operational resilience by integrating cyber, physical, and AI risk dimensions into one coherent model; and second, to support organisations in demonstrating accountability and preparedness in changing regulatory landscape. At the same time, the model has some limitations – it has not yet been empirically validated in real-world case studies and its implementation may be more feasible for larger, resource-rich entities than for smaller operators. Also, regulatory frameworks themselves and their interpretations and official guidelines continue to evolve, which means that the model should be understood as a conceptual and practical starting point rather than a definitive solution.

Following this, the paper introduces a practical, five-step model designed to help organisations do just that. Built on leading standards like ISO 28000 [16], ISO 28001 [17], ISO 31000 [18], ISO/IEC 27005 [19], ISO/IEC 27001 [20], and ISO/IEC 27002 [21] – and complemented by AI-focused frameworks, such as ISO/IEC 23894 [22], ISO/IEC 42001 [23], and the NIST AI Risk Management Framework [24] – model provides scalable and evidence-based approach for strengthening supply chain security. It's not only about meeting compliance; it's about building the kind of trust, transparency, security, and resilience that critical infrastructure demands in a digital age. This paper presents a starting point of a chosen areas of NIS2/CER/CRA-aligned five-phase model supported by practical and auditable documentation.

The main goal is to bridge the distance between regulatory duties and operational reality by offering a model that integrates cyber, physical, and AI risk dimensions into a single lifecycle. At the same time, it is important to acknowledge the limitations of the proposed

framework: it has not yet been validated through large-scale case studies, smaller operators may lack the resources to implement all its elements, there is a significant need for interdisciplinary expertise in implementation and the regulatory environment itself is still evolving and the model should therefore be seen as a starting point – as a conceptual and operational guide that invites further validation and adaptation in practice.

2. Operational Landscape and Risk Oversight in the EU Cybersecurity Framework

Cybersecurity in the EU is entering a new era, driven by the increasing interconnectedness of digital services, growing reliance on AI, and regulatory expansion. At the heart of this transformation lies growing awareness that critical infrastructure resilience is no longer determined solely by internal systems but by the robustness and visibility of the entire operational and supply ecosystem. This section explores the current state of readiness across the EU, based on ENISA's extensive reporting – and connects these insights with key scientific findings in the domains of cybersecurity governance, AI, and supply chain risk management.

European Union Agency for Cybersecurity's NIS360 2024 [25] report offers one of the most comprehensive overviews of cybersecurity maturity and sectorial criticality within the EU. The methodology evaluates 22 critical and essential sectors under the NIS2 Directive, revealing which sectors are lagging behind in maturity relative to their importance. Notably, sectors like IT service management, public administration, maritime transport, and healthcare fall into the so-called 'risk zone', where low maturity intersects with high criticality, signalling an urgent need for investment, guidance, collaboration, and audit. This imbalance is especially concerning, given the increased attack surface created by complex supply chains and third-party dependencies.

The supply chain itself is a major focus for ENISA – and its 2023 'Good Practices for Supply Chain Cybersecurity' [26] highlights several gaps between what's expected and what's practiced on the ground. Among the 1081 organisations surveyed, only 47% reported allocating dedicated budgets for IT/OT supply chain security and an even smaller number had assigned risk roles or formalised procedures for AI-related supplier assessments. This lack of preparedness leaves many essential and important entities vulnerable, not just to direct cyberattacks, but to supply-side compromises that cascade into broader infrastructure.

European Union Agency for Cybersecurity outlines actionable recommendations: organisations should map supply chain dependencies, apply secure-by-design procurement practices, require third-party audits, and classify AI components as potential attack vectors.

Another dimension of resilience introduced by ENISA is cyber stress testing. Originally borrowed from the financial sector, stress testing has now been adapted to cyber risk through *Handbook for Cyber Stress Tests* [27] published in May 2025. The methodology follows five stages: scoping, scenario design, execution, analysis, and follow-up. It provides practical way for operators of critical infrastructure to simulate high-impact cyber scenarios (which can be used also in testing AI-enabled ransomware or nation-state attacks tests on suppliers) and evaluate both system response and organisational coordination.

Building on ENISA's findings – scientific literature confirms that operational resilience is closely tied to governance structures – but also to clear mandates. Novelli et al. [28] argue that successful implementation of the EU AI Act [29] depends on strong institutional coordination between AI offices, national authorities, and scientific panels that provide transparent and expert-led oversight of AI risks. At the same time, Ruschemeier and Bareis [30] identify inconsistencies in member states' interpretations of key AI Act provisions as a barrier to harmonised operational responses.

While ENISA identifies structural gaps at the EU level, the authors' experience with operators in different EU countries confirms that these gaps manifest mostly and concretely in procurement processes, annexing supplier contracts, supplier monitoring, and the lack of clear accountability for AI tools. From author's experience, mid-tier providers often accept International Organization for Standardization (ISO)-aligned policies but fail to expose model lineage or data-handling paths for embedded AI features during audit and/or due diligence.

At the operational level, the misuse and/or poor oversight of AI models can introduce invisible risks. Collu et al. [31] demonstrate how (LLMs can behave unpredictably – and even override their own safety protocols if prompted adversarially – a trait exploitable in supply chain social engineering or prompt injection attacks. Mündler et al. [32] further expose the self-contradictory nature of hallucinated outputs which can lead to operational missteps if LLM-generated data is trusted without verification.

In dynamic and human–machine-integrated operations, *persona-driven* prompts (which simulate expert systems) pose another challenge. Kim et al. [33] caution that while personas may enhance task-specific accuracy – they also amplify cognitive biases and factual distortions in zero-shot reasoning tasks – which pose a great risk for any critical decision-making scenario in infrastructure operations.

Shojaee et al. [34] show that even advanced large reasoning models (LRMs) degrade under high-complexity tasks, risking unreliable outputs despite adequate resources. In critical infrastructure settings (where decisions often involve complex interdependencies) this creates operational risk. AI systems must therefore be paired with human oversight and safeguards to ensure reliability in high-stakes environments. Zhang et al. [35] points out that explainable AI frameworks are essential to bridge human oversight and machine autonomy in cybersecurity; ensuring that AI-generated actions can be interrogated and validated. Real-world examples of AI-aided decision-making in operational systems must therefore be assessed through explainability and auditability.

Beyond explainability, ENISA highlights that current AI systems (particularly those based on machine learning) remain vulnerable not only due to technical flaws but also due to the absence of consistent cybersecurity-specific standards [36]. The existing ISO 27000 series standards are relevant but insufficient on their own; AI-specific adaptations are needed to address issues, such as data poisoning, adversarial manipulation, and traceability of model components across the lifecycle.

The use of AI in monitoring and intrusion detection also opens new operational possibilities. Schmitt [37] finds that AI-enabled security can proactively detect malware and anomalies in smart infrastructure, but these systems also create operational dependencies that must be factored into risk and incident response planning.

As data becomes the lifeblood of operations, adversarial data inputs pose substantial threat. Both Laroche and Tachet des Combes [38] and Bharati and Podder [39] discuss risks emerging from data-influenced behavioural drift and manipulation in reinforcement learning and internet of things (IoT) systems; posing operational challenges in maintaining stable and predictable system behaviours.

European Union Agency for Cybersecurity in 2023 further identifies critical research needs in the 'AI and cybersecurity research' [40],

pointing out gaps in securing AI itself as distinct from using AI for cybersecurity. Among the top priorities are ensuring explainability and robustness in AI models, defending AI mechanisms against adversarial attacks and the development of datasets and benchmarks that reflect realistic and constantly evolving threats.

From a sectoral point of view, Yigit et al. [41] stress the importance of specialised benchmarks and test beds for evaluating generative AI and agentic models in critical infrastructure – arguing that without domain-specific validation – operational reliability cannot be guaranteed. Parallel to that, AI governance in high-risk industries, such as finance or tourism, must integrate risk controls related to multiple regulations, as emphasised by Botunac et al. [42], who suggest that AI must be evaluated not only on function but also on regulatory fit and compliance across systems and jurisdictions.

Operational readiness also requires awareness of the threat landscape. Hybrid threats (such as those leveraging disinformation or systemic uncertainty) were addressed by Akrap and Kamenetskyi [43], who emphasise that threat perception and identity-based targeting (as seen in Croatia and Ukraine) must be considered part of operational resilience. The hybridisation of cyber–physical threats has changed the battlefield, where operational sabotage may begin with soft vulnerabilities.

De Valk [44] highlights that the growing volume of unstructured data and the demand for real-time intelligence in protecting critical infrastructure require a shift towards augmented intelligence, where this analytic approach combines human reasoning with automated data processing to address analytic black holes and improve decision-making. In parallel, Akrap [45] warns that future attacks on critical infrastructure will be hybrid in nature – aiming to achieve information dominance through cyber space, with a focus on Information and communications technology (ICT), energy, and water–food systems. As such, effective protection depends not only on technology but also on the integration of intelligence and early detection of non-kinetic threat.

The EU cybersecurity strategy must therefore treat AI not only as a tool for automation but as a variable in the threat equation. This includes preparing for deepfakes and synthetic media manipulation, which was a concern raised by Meding and Sorge [46], who point out that EU institutions still lack a unified technical definition and detection standards for deepfakes under the AI Act.

Through CEN-CENELEC JTC 21 [47], EU is developing harmonised AI standards to support the AI Act [47], based on ISO/IEC 42001 and ISO/IEC 23894 (and other in ISO AI-related standards), but tailored to EU legal requirements. Although the process began in 2021, it has faced delays and key deliverables are still pending. The upcoming standards are expected to define more specific compliance mechanisms (especially for data governance and quality, robustness and cybersecurity, transparency, human oversight, and post-deployment monitoring). While awaiting finalisation, adopting ISO standards offers a strong interim foundation, but ongoing monitoring and alignment in EU-specific developments remain essential for compliance.

Beyond the cybersecurity and regulatory insights already discussed – broader academic perspective further illustrates the operational risks posed by unmanaged AI and data systems. Martin and Baccarani [15] describe the dual nature of AI in decision-making environments, emphasising that operational outcomes hinge on aligning AI behaviour with human oversight and governance values. From technical architecture perspective, Parlov et al. [49] emphasise that systems enabling lawful interception in telecom networks must be designed not only for compliance but also for resilience, given their dependency on structured and high-integrity data flows. Glerean [50] further underscores that AI systems managing personal data must embed privacy-by-design from the outset (particularly when operating in distributed or cloud-based environments), which is an essential prerequisite for securing operational continuity under EU data protection laws.

Only when critical infrastructure operations draw on these scientific insights (ranging from AI governance and adversarial threats to identity-centric targeting and operational test beds and many other challenges) – can the EU's vision of a truly resilient digital single market move from ambition to reality. What this vision ultimately requires is a shift towards modelling trough security-by-design & resilience-by-design – an approach where security and resilience are not treated as an optional safeguard but becomes a structural quality of systems and processes shown also from the point of view of secure and resilient supply chains, which ENISA and NIST frameworks continue to emphasise. In practice, this means that redundancy, transparency, adaptability, modularity, and the clearly defined targeted time to recover are considered as design criteria at the same level as efficiency or performance. It also means anticipating disruption as inevitable and shaping infrastructures that can absorb shocks and reconfigure under pressure while

delivering essential services despite adversity. Rather than patching weaknesses after crises, mentioned modelling seeks to cultivate robustness from the very beginning (in technical architectures, governance arrangements, etc.) and in the everyday culture of organisations that operate Europe's most critical assets.

3. Strategic Role of Supply Chains in Security and Resilience of Critical Infrastructure

Security and resilience of critical infrastructure can no longer be reduced only to physical protection or digital hardening of core systems. A considerable part of systemic exposure now originates in the supply chains that sustain, operate, maintain, and digitally enable essential services. Across energy, transport, water, healthcare, and communications – these sectors rely on extended networks of third-party providers that crossborders and deliver everything from OT components and IoT sensors to specialist services, proprietary software, human expertise, and cloud services. Now taking into account this ecosystem, the concept of the internet of everything (IoE) becomes particularly relevant – a paradigm embracing not only connected devices, hardware, and software but also the people, procedures, processes, and data flows between them.

At the same time, these same supply chains are becoming the most vulnerable and exploited layer in the modern threat landscape. Threat actors increasingly shift their focus to suppliers, subcontractors, and software providers as entry points into highly secured systems. This 'attack by proxy' strategy has been evidenced in numerous incidents, where compromise of a seemingly peripheral supplier resulted in national-level disruption. The mentioned incidents are strong reminders that supply chain compromise is not hypothetical but systemic and if poorly managed can act as a force multiplier of cascading failures across entire sectors.

According to the authors' fieldwork with critical infrastructure providers, even seemingly peripheral suppliers (in example cleaning services, CCTV, HVAC, or smaller IT contractors) have proven to be weak points in practice – frequently retained badge access or unmanaged remote accounts, which become material during crisis escalation.

Supply chain risk management is not a peripheral activity but a core pillar of infrastructure's both security and resilience. Failure to adequately identify, evaluate, and mitigate risks across the supply chain

undermines even the most mature internal security controls. Even a single unassessed supplier, an insecure software component, the unrecognised subcontractor, or a subcontractor without cyber hygiene may serve as the weakest link that collapses an entire system. Here, the notion of security culture becomes critical. It is more than technical standards or compliance checklists because it reflects everyday attitudes and leadership priorities which can easily be shown through a degree of awareness across an organisation and its suppliers. When companies treat cybersecurity as an afterthought, neglect timely patching, avoid transparent incident reporting, or ignore staff training – they quietly introduce vulnerabilities into the wider ecosystem. On the other hand, where security culture is strong, suppliers are more open, collaboration between partners is encouraged, leaders make resilience, a visible priority and responsibilities are shared across departments, rather than isolated in IT units. In such an environment, a well-governed supply chain becomes a real strategic asset by enabling quicker recovery, reliable redundancy, and continuity of essential services even under geopolitical tension, economic or social volatility, or complex hybrid threats.

4. Role of the NIS2, CER, and CRA in the EU Strategic Framework

The EU has taken a strong stance on strengthening the resilience of critical infrastructure by introducing two complementary regulatory pillars: the NIS2 Directive and the CER Directive. While NIS2 (Directive (EU) 2022/2555) focuses on cybersecurity (especially in the context of digital systems and supply chains), CER Directive (Directive (EU) 2022/2557) broadens the lens to include all types of risks – ranging from cyber threats to physical disruptions, natural hazards, terrorism, and even hybrid attacks that combine multiple threat vectors.

Together, these directives signal a fundamental shift from compliance-based security towards proactive and operational resilience. NIS2 requires essential and important entities to manage digital risk across their supply chains, ensuring security is built into procurement, partnerships, and third-party services, while CER goes a step further by demanding that critical entities assess and prepare for any threat that could disrupt the delivery of essential services (whether it's a cyber incident, flood, power outage, or geopolitical tension affecting upstream suppliers).

What's clear is that resilience goes far beyond technical defences or backup systems – it is about understanding dependencies,

recognising weaknesses and vulnerabilities across complete network of not only systems but interested parties having visibility into who and what you rely on and being ready to respond when something (anything!) goes wrong. This aligns with the EU's broader ambition for secure and trustworthy digital single market, where resilience is not an afterthought but also built-in feature of how essential services are delivered and protected.

In this light, supply chain security becomes both a legal obligation and a strategic imperative – a way to protect not just IT systems but the social, economic, and physical infrastructure we depend upon every day.

The EU has established a regulatory framework composed of multiple instruments that collectively shape resilience across digital infrastructure, physical systems, risks arising from access rights management, and technological products. Core instruments include the NIS2 Directive (Directive (EU) 2022/2555), CER Directive (Directive (EU) 2022/2557) and the Cyber Resilience Act (Regulation (EU) 2024/2847). These are reinforced by additional acts, such as Digital Operational Resilience Act (DORA) [51] for financial services, Artificial Intelligence Act [52], which introduces a risk-based model for AI systems, and in certain domains by sector-specific regimes overlapping with safety, security, and critical infrastructure. The interaction of these measures demonstrates that the EU is constructing not a single uniform rule but a layered set of requirements addressing entities, services, products, and emerging technologies simultaneously which poses a complex interdisciplinary requirements and experts' knowledge when seen from an compliance and harmonisation point of view.

NIS2 prescribes cybersecurity and risk-management duties for essential and important entities, with emphasis on governance, awareness, testing, supply chain oversight, and reporting of major incidents. CER extends the coverage to physical, natural, and all kinds of hybrid threats capable of disrupting essential services, regardless of their digital origin. CRA creates obligations for manufacturers and distributors of products with digital elements by requiring secure design, vulnerability management, markings, and sustained update practices to prevent systemic weaknesses in hardware and software. DORA imposes resilience rules for financial actors, compelling them to withstand ICT disruptions and ensure continuity of critical financial operations. AI Act applies to all AI systems through a graded approach: it (1) prohibits certain 'unacceptable-risk' practices, (2) establishes strict conformity requirements

for 'high-risk' applications in domains, such as infrastructure, education, and law enforcement, and (3) introduces transparency obligations for 'limited-risk' uses – while leaving minimal-risk systems largely outside regulatory scope. Seeing in parallel, sectoral legislation in transport, energy, food, or health adds further resilience and safety obligations – which make the regulatory environment more complex than an 'usual' three-pillar structure.

Together, these instruments redefine resilience: no longer a checklist but a distributed obligation across organisational, infrastructural, technological, and sectoral layers, with clear duties for testing and measurement. Instead of focusing exclusively on firewalls, backup systems, or incident reporting – the framework requires mapping dependencies, securing components at the product level, analysing vulnerabilities in supply chains, and embedding resilience into governance and operational structures. The result is a regulatory setting where continuity of services, integrity of products, trust in digital technologies, and preparedness against systemic disruption are treated as mutually reinforcing requirements of the European economic and social environment.

5. AI: New Frontier of Risks and Opportunities in the Critical Infrastructure and its Supply Chains

As organisations modernise critical infrastructure operations, the integration of AI into both core infrastructure and its supporting supply chains presents a dual-edged transformation. On the one hand, AI enables predictive maintenance, real-time anomaly detection, autonomous response mechanisms, and optimisation of energy and logistics networks – making infrastructure more efficient, adaptive, secure, and resilient. In supply chains, AI might improve supplier risk scoring, dynamic rerouting, fraud detection, procurement intelligence, etc.

But on the other hand, AI also amplifies new classes of threats. Supply chains become vulnerable to AI-driven attacks (such as deepfake-based social engineering, large-scale automated scanning for vulnerabilities, and manipulation of data-driven decision systems). Given that – data integrity risks, adversarial machine learning, and opaque AI supply chains (e.g. sourcing unverified machine learning models or training data, exposing the data through different AI agents; or just being unaware of adapting necessary settings related to prohibiting uploaded data to be used for training and/or improving the algorithm for the public) introduce entirely new risk vectors.

Thus, while AI enhances capabilities, it must be accompanied by responsible risk governance frameworks, such as the NIST AI Risk Management Framework, ISO/IEC 23894 (AI risk), and ISO/IEC 42001 (AI management systems), ensuring that innovation does not outpace assurance. In supply chain contexts, this includes verifying the security of AI models used by suppliers, monitoring AI-generated outputs, and securing training pipelines from tampering.

As Europe moves towards a resilient, digital, and interconnected future, the security of critical infrastructure will be judged not only by its firewalls and physical barriers but by the integrity, transparency, and trustworthiness of its supply chain ecosystems and the AI systems it embeds. The intersection of regulatory reform (NIS2/CER/CRA), standards-based frameworks (ISO 28000/28001), and AI risk management will define the next generation of critical infrastructure protection.

6. Value of Data, Criticality Classification, and Risks of Exposure in the Supply Chain

Data powers every aspect of infrastructure, from the flow of electricity and water to the optimisation of transport logistics and real-time healthcare coordination. It is no longer just a byproduct of systems – it is what makes them function.

In this context, understanding the value of data and managing its exposure across the supply chain is essential for protecting not only the infrastructure itself but also the societal and economic stability it supports. Supply chain is not only a channel for materials and services but it is also a conduit through which (sensitive) data flows continuously. This includes configuration settings, supplier schedules, AI training inputs, system telemetry, incident reports, etc. With each new integration point, especially with third parties and AI-based tools – comes another opportunity for data to be leaked, blocked, tampered with, and other threats. To manage these risks, organisations must begin with a clear classification of data criticality [53]. Not all data carries the same weight – and some datasets (such as real-time operational control commands or credentials used to manage AI-driven systems) are foundational to safety and continuity. These are 'mission-critical' data assets. Others, such as predictive maintenance schedules or supplier delivery forecasts, may be less immediately sensitive but still vital to long-term resilience. Data must be classified based on its relevance to the continuity of essential services, its confidentiality requirements, and its role in decision-making.

Unfortunately, in praxis, in many supply chain environments, this classification is either absent or inconsistently applied. This leaves infrastructure vulnerable to three primary forms of data exposure: leakage, unavailability, and manipulation.

Data leakage often stems from misconfigured supplier systems, insecure APIs, or human error. It can lead to the exposure of sensitive operational data, including facility layouts, control system logic, or AI model configurations. Such leaks don't just invite espionage but they enable attackers to map, understand, and exploit infrastructure remotely.

Data unavailability (typically caused by ransomware or intentional denial-of-service attacks) can cripple services by encrypting operational data or making it inaccessible. In supply chains, this might mean blocking supplier orders, disabling access to digital twins or model forecasts, or freezing remote monitoring functions. When AI systems depend on this data to make predictions or automate responses, such disruptions can have significant and hard-to-stop cascading effect.

Perhaps, today the most underestimated risk is *data manipulation*. As Esterajher and Mihaljević observe in the context of societal dynamics, manipulation undermines trust and creates systemic fragility [54]; the same logic applies in technical environments where data integrity is quietly eroded. It can appear in many different forms – from the quiet introduction of fabricated records into operational systems to the silent removal of entire datasets or the gradual alteration of values that slowly undermines integrity over time. In practice, this might mean falsified sensor readings that distort situational awareness, supplier updates that are tampered with before reaching procurement systems, training data that is deliberately poisoned so that AI models begin to misclassify or drift in ways that escape normal checks, and many more technology-related challenges because of everyday evolving possibilities. The danger is that even small, *almost invisible changes accumulate* until they reshape the behaviour of systems and decision-making processes. In environments that increasingly rely on automation and AI, such manipulations are magnified: models respond to poisoned inputs, predictive tools start to produce misleading forecasts, and security monitoring loses the ability to separate truth from deception and all of that hard to recognise in early phase. When AI components or datasets are sourced from external vendors, the risk deepens further and evolves, because operators have little visibility into how those datasets were built, maintained, hosted, or

protected. In these circumstances, data manipulation is not just an operational disruption but it corrodes trust, weakens accountability, weakens security in potentially large scale, and erodes the resilience on which critical infrastructure ultimately depends.

In this way, AI does not merely introduce new risk but it magnifies existing vulnerabilities in the supply chain. It creates new points of dependency and new targets for attackers. AI systems are only as trustworthy as the data they are trained on, the environments in which they operate, and the suppliers who build or maintain them. If that ecosystem is compromised, the integrity of AI decisions (on everything from procurement to crisis response) cannot be assured.

Therefore, any serious approach to supply chain security must include a *data-centric strategy*. This means:

- classifying data based on its operational criticality and AI dependencies;
- mapping where and how data flows through the supply chain, including through AI models;
- enforcing access controls, encryption, and integrity verification mechanisms tailored to data type and context;
- auditing not only the suppliers themselves but also how they handle your data, train their models, and detect data tampering;
- monitoring AI outputs for signs of anomalous or adversarial behaviour, specially in shared supply ecosystems.

In the age of smart infrastructure, protecting supply chains means protecting the data that flows through them. A leak, block, or manipulation of that data is no longer just an IT issue but it is an operational incident that can threaten lives, public trust, and national resilience. When data governance and AI risk management are integrated into the core of supply chain strategy, critical infrastructure organisations are better equipped to anticipate, absorb, and respond to the digital threats of the 21st century and connectivity of different devices – business and personal.

7. International Standards and Frameworks in Operationalisation

The model discussed in this paper was not conceived as an isolated academic construct but as a deliberate attempt to weave together a body of international standards and governance instruments that, over the past decades, have conditioned how

organisations conceptualise risk, implement security measures, and maintain operational continuity. The intention was not to simply transpose clauses from ISO catalogues but to create a framework that can operate within the existing management systems, withstand scrutiny in regulatory settings where accountability is demanded, and remain intelligible to compliance implementators, auditors, regulators, and practitioners who navigate multiple overlapping obligations. The act of merging distinct standards into a single architecture was not an exercise in convenience but a necessity: each on its own falls short, yet taken together, they form a fabric capable of covering areas – such as artificial intelligence vulnerabilities – that would otherwise remain exposed.

Among the standards incorporated, those addressing supply chain security were given particular weight. ISO 28000 and ISO 28001 are not treated as abstract reference points but as guides that influence supplier evaluation, logistics continuity, and the mapping of interdependencies that often remain invisible until disruption makes them tangible. Building on this base, ISO/IEC 27001 and ISO/IEC 27002 bring the structure of information security management systems and the granularity of specific controls, while ISO/IEC 27005 introduces methodological rigour in the analysis, assessment, and treatment of risk.

Yet the terrain of contemporary infrastructure cannot be charted with these instruments alone. AI introduces a category of exposures of a different order: manipulated models, poisoned data, silent drift in performance, the opacity of training regimes, and the absence of explainability in outputs. To confront these conditions, the model deliberately incorporates ISO/IEC 23894 as a guide for AI risk management, ISO/IEC 42001 as the first full management system for AI governance, and the NIST AI RMF for its pragmatic structure and attention to adversarial scenarios. Together, this ensemble does more than echo the existing obligations: it sketches a path forward in which compliance and foresight intersect, enabling organisations to meet today's requirements while preparing for tomorrow's uncertainties.

The authors' experience in applying ISO standards and regulatory harmonisation of technical and organisational measures in different critical infrastructure sectors showed that operators frequently adapt the documentation formally but the challenge lies in embedding these requirements into everyday practice. And as most pinpoints in security challenges, key success factor of using the model will depend on the level of operationalisation and tracing

its maturity level in an objective way, and not only generating the documentation.

8. Five-step Supply Chain Security and AI Risk Governance Model for the Critical Infrastructure under NIS2, CER, and CRA

8.1. Methodology

The formulation of the five-step supply chain security and AI risk governance model was the outcome of a methodological process that sought to combine pragmatism with conceptual rigor, not by inventing an entirely novel architecture but by weaving together the existing best practices, binding regulatory obligations and insights drawn from the expanding body of research on critical infrastructure resilience in order to produce a framework that is operationally coherent and realistically applicable to entities falling within the chosen scope of the NIS2, CER, and CRA. The starting point was a comparative examination of international standards and guidelines that have gradually shaped the discourse and practice of supply chain security and risk governance. We prioritized ISO 31000 because risk criteria could be agreed across legal, operations, and OT; we used ISO 28000/28001 where supplier tiering and logistics continuity were dominant; and we adopted ISO/IEC 23894/42001 only where AI inference or training materially affected service continuity.

ISO 31000 was treated as the structural backbone, not because it offers readymade prescriptions but because its cyclical approach to context definition, risk identification, analysis, treatment, and iterative review has become a *lingua franca* for risk professionals across jurisdictions. To give the framework specific traction in the supply chain domain, ISO 28000 and ISO 28001 were scrutinised for their concrete provisions on supplier oversight, continuity of logistics, and dependency mapping, while ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27005 were integrated to situate the model within the established discipline of information security/cybersecurity management – bringing with them the structure of management systems, catalogues of organisational and technical controls, and risk assessment methodologies already recognised in the context of regulatory compliance.

A further methodological decision was to incorporate AI into the model from the outset, since it was evident that the traditional security standards (comprehensive as they are in their own field) do

not sufficiently account for vulnerabilities specific to AI ecosystems: adversarial manipulation of models, silent drift in system behaviour, poisoning of training datasets, opacity in the provenance of inputs, and the lack of transparency in decision outputs. To respond to these deficits, ISO/IEC 23894 was adopted as the first global guidance on AI risk management, ISO/IEC 42001 as a framework for governance of AI systems at the organisational level, and the NIST AI risk management framework as a practice-oriented guide with explicit attention to adversarial scenarios. The mapping of these instruments was undertaken not as a mechanical exercise but as a judgement about regulatory alignment, operational feasibility, and conceptual coherence, with the recognition that while regulations oblige entities to exercise oversight over their third parties and the AI Act lays down general duties for high-risk systems, neither currently offers harmonised operational guidance for the intersection of AI and supply chains. The proposed model addresses precisely this lacuna by embedding AI risk considerations into every stage of the lifecycle.

The derivation of the five steps was therefore neither linear nor superficial but iterative and layered. Established risk management cycles were revisited, standards compared across domains, ENISA's recommendations introduced where they brought sectoral clarity and the more recent practice of cyber stress testing considered as a means of exposing systemic weaknesses. Each phase of the model was deliberately shaped to incorporate not only the expected technical and organisational components/measures but also hybrid threats, geopolitical pressures, environmental hazards, and the vulnerabilities inherent in data flows. Thus, the phase of identifying and assessing risks is extended beyond supplier reliability and IT/OT weaknesses to encompass AI model assurance, while the review and improvement phase moves beyond conventional auditing to include longitudinal monitoring of algorithmic bias, model drift, and other unintended behaviours.

Model was conceived with dual applicability. For large and complex operators of essential services it offers a detailed framework capable of documenting compliance, while for medium-sized or resource-constrained entities, it remains adaptable through selective implementation, reliance on standardised audit checklists, or the outsourcing of specialist AI assurance tasks.

Although empirical validation through case studies has not yet been conducted, the model's grounding in internationally recognised standards, reinforced by AI-specific safeguards and aligned with EU

regulatory trajectories, lends it credibility as both a conceptual contribution and a practical roadmap for closing the gap between compliance and resilience in a more and more AI-driven supply chain environment. The environment that should be constantly taken with higher attention.

8.2. Role of Plan-do-Check-Act (PDCA) Cycle

The standards that form the backbone of the proposed model are bound together by structural logic that is neither incidental nor decorative but fundamental: their reliance on the PDCA cycle. In practical terms, this is not just a theoretical construct but a working rhythm familiar to anyone involved in continuous improvement. This cyclical pattern, developed originally in the field of quality management and subsequently absorbed into risk management, has endured precisely because it converts the often abstract ambition of continual improvement into a disciplined sequence of actions, which in turn makes the standards not only auditable by external parties but also sustainable in everyday organisational practice. Within this logic, the stage of planning is not confined to producing a static document but encompasses the definition of organisational context, the articulation of regulatory obligations as they apply across jurisdictions, the mapping of interdependencies that stretch beyond the immediate enterprise, and the scoping of risks in ways that can be tested against both historical experience and evolving threat landscapes. In other words, planning here becomes an exercise in organisational self-awareness and not just another simple documentation. The stage of doing brings these abstractions into concrete form: contractual clauses that translate resilience into legal obligations, technical and procedural safeguards that condition daily operations, measures that cultivate redundancy or modularity in supply chains, and requirements that extend specifically to AI components – whose vulnerabilities cannot be treated as afterthoughts. At this point, it could be seen that strategies turn into routines, and policy statements begin to shape behaviour.

When the cycle moves into the checking phase, the concern shifts from design to scrutiny: the monitoring of supplier performance in real time, the auditing of AI system outputs for signs of drift or manipulation, the execution of stress tests that reveal weaknesses under extreme scenarios, the simulation of hybrid threats that combine physical disruption with digital deception, and the rehearsal of multi-domain incident responses that expose not only technical fragilities but also organisational blind spots. This is the

phase where assumptions are tested, and reality checks in – which can sometimes show some dissapointing areas. At the end, the acting phase closes the loop, not through ritual but through processes that compel organisations to confront their shortcomings: periodic audits that are more than box-ticking, management reviews that surface strategic misalignments, the systematic revision of risk registers, the introduction of resilience metrics capable of tracking progress or decline, and the translation of lessons learned into updated roadmaps that influence both governance structures and operational practices. The value of this stage lies in its honesty – it forces reflection and adaptation rather than "plain" compliance.

This PDCA cycle was deliberately retained in the model not as a mere homage to the existing practice but as a structural choice designed to anchor the framework in forms already recognisable to critical infrastructure operators. Its persistence reflects both practicality and trust: people tend to work best within systems they already know how to navigate. The familiarity to practitioners accustomed to ISO 27001, ISO 28000, and related standards increases the likelihood of adoption, yet its significance lies in the way it has been extended: the same cyclical logic that has long governed information security and supply chain management is here projected onto domains that include AI risk governance, data-centric vulnerabilities, and the multifaceted pressures of hybrid threats. In doing so, the PDCA cycle functions not only as a management mechanism but as a methodological bridge, one that links established security practices with emerging challenges, and allows continuity without ignoring the discontinuities introduced by new technologies and geopolitical realities.

In the authors' practical engagements – many organisations stop at the 'Plan' and 'Do' phases, while the 'Check' and 'Act' phases are neglected, often misunderstood or have just been ignored, a pattern that is as common as it is risky, leaving controls untested and resilience overstated, so the security and resilience 'success rate' depends again on the clear operationalisation and not only documentation. Put simply, without the discipline to close the loop, improvement remains an illusion.

8.3. Limitations

While the model proposed in this paper provides structured and practical framework for managing supply chain and AI-related risks under NIS2, CER, and CRA – several limitations need to be acknowledged. These limitations do not undermine the

relevance of the model itself but highlight the boundaries within which it should be interpreted and applied.

1. Model is based on a synthesis of international standards, EU regulatory requirements, scientific literature and author's practical experience in wide scope of sectors but it has not yet been empirically validated through series of monitored case studies or industry pilots. This means that its practical effectiveness still depends on future application and feedback from critical infrastructure operators. Without such real-world testing – certain recommendations may remain theoretical or overly ambitious in organisations with limited resources.
2. Model assumes a level of organisational maturity that is not uniform across all entities covered by NIS2, CER, and CRA. Large operators with established security and compliance teams may find the five steps compatible with their existing processes and not so resource-heavy, while medium-sized or resource-constrained entities may struggle to operationalise all elements at once which points to a need for a selective adoption and gradual implementation dependable on the context of organisation, but the model does not yet provide a detailed roadmap for scaling down.
3. Regulatory environment itself is still evolving. NIS2, CER, and CRA are in the different stages of the process and the AI Act is at an early stage of implementation (and partial). The forthcoming secondary legislation, technical standards under CEN-CENELEC, and sector-specific guidance may alter the expectations placed on organisations. With that in mind, the model reflects the state of the regulatory landscape at the time of writing but may need updates and continuous assessments of upcoming obligations.
4. Integration of AI-specific risk management is a moving target highly dependable on understanding the scope of AI used and its life cycle within an organization. Standards such as ISO/IEC 23894 and ISO/IEC 42001, as well as the NIST AI RMF, are relatively recent and continue to develop in response to new vulnerabilities and practices. The model incorporates the best available references but AI-related threats and opportunities evolve rapidly and may outpace the safeguards currently defined in these frameworks. Not less important – the competence in understanding the standards and organisation's ability to oversee the AI in a multidisciplinary way plays a crucial role.
5. Model focuses on governance structures (documentation and control processes) which are necessary for compliance and resilience. It is important to state that it does not address in depth the cultural and human factors that often determine the

success or failure of security initiatives (such as organisational security culture, as stated before - cross-departmental collaboration, willingness of suppliers to accept new contractual obligations which today poses one of the most challenging areas, or the level of the understanding of new regulatory requirements). These socio-technical dimensions are acknowledged but they fall outside the immediate scope of this paper and warrant further research.

The model should be understood as a conceptual and operational starting point, but not as a definitive solution since all organisations are different. Its value lies in providing structured pathway for aligning supply chain and AI risk management with regulatory requirements but its long-term utility depends on empirical validation, iterative refinement, possible regulatory-related interpretation changes, and adaptation to the specific realities of critical infrastructure sectors – based not only on technological areas and refinements but heavy dependable on human factor itself.

8.4. Five-Step Supply Chain Security and AI Risk Governance Model

The five-step supply chain security and AI risk governance model for the critical infrastructure provide a clear, actionable framework for identifying, treating, and governing risks in the supply chain – drawing on international best practices from chosen ISO standards and frameworks. The model is designed to be both comprehensive and scalable, supporting organisations of varying sizes and complexities, while ensuring alignment with NIS2/CER/CRA requirements.

Each of the five steps in the model reflects a critical phase in the supply chain risk lifecycle and engages different levels of the organisation – from executive leadership to operational and technical teams.

The five-step model with the organisational levels and involvement needs is provided below:

1. *Define context and scope* – This step requires top management and risk governance teams to define the organisation's supply chain ecosystem, regulatory obligations and security boundaries, non-digital threat exposure mapping, and cross-sector dependencies. It sets the foundation for accountability and determines the focus of all subsequent actions

2. *Identify and assess risks* – Risk managers, procurement leads, cybersecurity analysts, and compliance officers collaborate to identify vulnerabilities in supplier relationships, third-party technologies and AI systems, and climate, political, and physical risk vectors – it is a joint effort across business, technical, and legal domains.
3. *Treat risks and implement controls* – Procurement units, contract managers, chief information security officers (CISOs), and legal advisors work together to ensure that appropriate security requirements are embedded in processes and agreements, with resilience controls beyond cybersecurity (e.g. dual sourcing, alternative logistics) – its control decisions are based on impact and feasibility and often require executive sign-off for high-risk suppliers or AI applications or high risks related to resilience factors.
4. *Monitor, operate, and prepare for incidents* – Led by corporate security, physical and cybersecurity operations, IT departments, supplier managers, and business continuity teams, and supported by crisis communication units, it involves the practical execution of monitoring activities, incident reporting procedures, communication procedures, and coordinated response protocols (it includes hybrid threat scenarios tested through tabletop exercises and AI-driven simulations, integration of environmental and geopolitical early warning systems, supplier readiness checks for multi-domain disruptions, forensic visibility into AI anomalies triggered by real-world events as well as structured communication with regulators and oversight bodies. Also, equally important is the ability to inform the public and affected stakeholders through clear crisis communication strategies, ensuring timely, credible, and consistent messaging that preserves trust, manages reputational impact, supports decision-makers, and prevents the spread of misinformation during large-scale incidents.
5. *Review, audit, and improve* – Internal audit functions, executive leadership, and governance bodies assess performance, oversee external audits, and drive continual improvement – this is where strategic oversight meets operational learning, ensuring that risks remain visible and addressed over time, including resilience metrics and regulatory reporting needs.

The strength of this model lies in its balance between strategic alignment and operational execution, enabling organisations to demonstrate compliance, build trust, and increase resilience. It ensures that security and risk management are not siloed functions but shared responsibilities across departments and leadership levels.

Most importantly, it prepares critical infrastructure entities not just for known risks but also for emerging threats – particularly those stemming from AI integration and supply chain interdependence.

In applying this model, organisations create not just a barrier to disruption but a pathway to long-term operational integrity and regulatory confidence in an evolving European cybersecurity landscape.

Following this strategic overview, the next section presents the five-step supply chain risk and security model in detail. Each phase of the model builds logically on the previous, offering a structured yet adaptable approach for organisations seeking to operationalise risk governance across their supply chains while aligning with the NIS2, CER, CRA, and international standards.

The model is designed not only to address compliance requirements but to embed resilience into the operational fabric of critical infrastructure entities. It connects high-level governance with frontline implementation and provides practical, evidence-based tools for managing risks associated with suppliers, technologies, and AI-enabled processes.

Explanation of the model:

Step 1: Define context and scope
First step in securing the supply chain is understanding where your organisation fits in a wider ecosystem of partners, technologies, and services. This means looking beyond internal operations and mapping out how third-party suppliers, contractors, and technology providers – especially those using AI – connect to your critical services.

To do this effectively, organisations should build a detailed overview of key supply chain dependencies, identifying which services rely on external partners and where AI plays a role. A 'statement of application' (e.g. in line with ISO 28001) helps formalise what parts of the supply chain fall under your security program. It's equally important to maintain a register of legal and regulatory requirements, especially those under the NIS2, CER, and CRA, so that your obligations are clear. Keeping an updated inventory of AI usage within your supply chain will highlight any specific risks tied to automated systems and/or hybrid threats – and help shape future oversight. Introduce a critical entity dependency map and threat landscape overview combining digital and non-digital exposures (including climate, terrorism, and hybrid threats).

Evidences to be sought and their purpose:

- *Supply chain context and dependency map* – Identifies critical internal processes and their upstream/downstream dependencies, including IT/IoT/OT, and AI vendors; establishes visibility over essential connections, and map interdependencies across sectors (e.g. energy providers supporting healthcare).
- *Exposure* – Defines geographic and logistical exposure to natural hazards and human-caused threats.
- *Regulatory/contractual requirements register* – Links relevant laws, directives (e.g. NIS2/CER) and contractual obligations to supply chain segments, ensuring legal compliance; establish a register of security and resilience obligations under national transposition laws.
- *AI use inventory in the supply chain* – Catalogues where AI systems are used, by whom and for what purposes; provides the basis for assessing AI-specific risks and exposures.

Step 2: Identify and assess risks

Once the scope is defined, the next step is to identify which parts of your supply chain pose real risk. This involves looking at both known threats and emerging vulnerabilities – whether they come from software, logistics, service providers, or AI-based tools used by your suppliers.

Comprehensive risk register should bring all these factors together. It acts as a single source of truth, capturing everything from hardware weaknesses to supplier reliability issues and AI model exposures. Risk assessments and threat modelling exercises help you understand what could go wrong and where. Profiling your suppliers – based on how critical they are, how mature their security is, and how exposed they are – lets you prioritize. And for AI-specific tools, model assurance reports help determine how transparent, safe, and trustworthy those systems really are.

Evidences to be sought and their purpose:

- *Supply chain and AI risk register* – Serves as a single, auditable source of documented risks related to suppliers, components, data flows and AI models, and non-cyber scenarios (e.g. fuel shortages, heatwave disruptions).
- *Threat and vulnerability assessments* – Provides justification for controls based on real-world threat scenarios; supports risk quantification.
- *Supplier risk profiles* – Categorises suppliers by criticality, compliance posture, and exposure to threats; enables prioritization of oversight and resources.

- *AI model assurance reports* – Documents explainability, robustness, and testing status of AI systems used in or by the supply chain; supports trust and traceability.
- *Scenario-based assessments* – Using ENISA's cyber stress testing adapted for hybrid threat simulations.

Step 3: Treat risks and implement controls

With a clear understanding of the risks, the next step is deciding how to manage them. This involves defining practical controls – some technical, some contractual, and some procedural – to reduce your exposure to acceptable levels.

This might mean adding physical security, resilience, and cybersecurity clauses to supplier contracts, such as supplier diversification, and also requiring AI models to be auditable or updated regularly. You'll also want a specific plan for managing AI risks – things like defending against data manipulation or ensuring that models don't 'drift' into inaccurate or biased decision-making. Mapping each risk to a clear action, responsible person and timeline make up your risk treatment plan. At the end, the procurement process itself should be refined to make sure new suppliers are evaluated for security before they come on board – not after something goes wrong.

Evidences to be sought and their purpose:

- *Supplier security requirements (contractual clauses)* – Specifies minimum security controls (including for AI) in contracts and SLAs; provides enforceable security obligations.
- *AI risk mitigation plan* – Details technical and procedural measures to mitigate AI-specific threats, such as model drift, poisoning, or adversarial input.
- *Risk treatment plan* – Aligns each identified risk with an assigned control, owner, and timeframe which supports accountability and tracking of risk response.
- *Secure procurement procedures* – Embeds risk-based evaluations in supplier selection, on boarding and renewal; ensures suppliers meet your security and resilience standards from the start; consider supplier diversification, physical security checks, and emergency logistics protocols.

Step 4: Monitor, operate, and prepare for incidents

Having controls in place is just the start; resilience depends on continuous monitoring, coordinated operations, and readiness for incidents. This function is typically led by corporate security, physical and cybersecurity operations, IT departments, supplier managers,

and business continuity teams, supported by crisis communication units. It involves executing monitoring activities, applying incident reporting procedures, managing communication lines, and activating coordinated response protocols.

Resilience in this step requires testing hybrid threat scenarios through tabletop exercises and AI-driven simulations, integrating environmental and geopolitical early-warning systems, verifying supplier readiness for multi-domain disruptions, and maintaining forensic visibility into AI anomalies triggered by real-world events. A structured approach to communication with regulators and oversight bodies is equally important, as is the ability to inform the public and affected stakeholders. Effective crisis communication strategies ensure that messaging remains timely, credible, and consistent, preserving trust, supporting decision-makers, managing reputational impacts, and preventing misinformation during large-scale incidents.

Evidences to be sought and their purpose:

- *Supply chain security plan* – Documents operational roles, responsibilities and incident-handling procedures across organisational and supplier functions; ensures coherent execution under pressure.
- *Supplier-monitoring dashboard* – Provides real-time or periodic data on compliance, performance, threat indicators, and AI system behaviour; supports situational awareness and early detection.
- *AI output audit logs* – capture anomalies, automated decisions, and system behaviour; enable forensic investigation, traceability, and compliance in regulated environments.
- *Joint incident response protocols* – Define coordinated response roles and channels with suppliers, regulators, and emergency services; ensure readiness for shared scenarios, such as cyber incidents, natural hazards, or hybrid threats.
- *Testing and simulation records* – Evidence of drills, tabletop exercises. and AI-driven simulations; validate that response plans remain functional against multi-domain disruptions.
- *Crisis communication playbooks* – Structured procedures for engaging oversight bodies, regulators, public, and affected stakeholders; ensures consistent messaging, trust preservation, and reputational protection during incidents and recovery/back-to-normal state.

Step 5: Review, audit, and improve

No system stays secure on its own. The final step is about closing the loop – reviewing how well your supply chain risk program

is working and adjusting it as threats, technologies, and suppliers evolve.

Regular audits (both internal and those involving suppliers) provide critical insight into what's working and what's not. Management reviews give senior leaders a chance to weigh in and stay accountable, which is an expectation under both ISO 28000 and NIS2, CER, and CRA. In AI-heavy environments, ongoing checks for bias, drift, and unintended behaviour in models help to reduce both ethical and operational risks. Keeping your risk registers and strategic roadmaps updated means you're staying ahead of future problems. And finally, conducting periodic assessments of your compliance with NIS2/CER/CRA shows that your organisation is not only meeting the letter of the law but also actively managing the spirit of resilience behind it.

Evidences to be sought and their purpose:

- *Internal and supplier-facing audit reports* – Demonstrates whether implemented controls are functioning; identifies systemic gaps and improvement opportunities and integrates resilience maturity metrics into internal and external audit cycles.
- *Management review records* – Shows active executive engagement in overseeing risk governance, fulfilling regulatory and ISO leadership requirements.
- *AI model bias reports* – Evaluates ongoing accuracy, fairness, and reliability of machine-learning systems; essential for legal defensibility and ethical integrity.
- *Updated risk registers and strategic roadmaps* – Reflects changes in supplier landscape, technologies, or threat intelligence; shows that governance is dynamic and forward-looking.
- *NIS2, CER, CRA, and related national implementing laws compliance assessment results* – Document the organisation's status against national-level NIS2/CER/CRA transposition/implementing laws; provide readiness for external review or enforcement.

9. Conclusions

The digital transformation of critical infrastructure brings clear benefits as well as new vulnerabilities. Supply chains, once treated as peripheral considerations, have emerged as central determinants of resilience. Incidents ranging from ransomware campaigns to the compromise of trusted software libraries and AI model repositories show how attackers exploit weak points in supplier networks and propagate disruption across entire sectors. For

critical infrastructure, such events do not remain isolated breaches; they ripple outward, destabilising energy distribution, food, healthcare delivery, transport safety, and public trust.

This paper addressed these challenges by presenting a five-step supply chain security and AI risk governance model tailored to chosen NIS2, CER, and CRA requirements. The model is grounded in the PDCA logic of ISO 31000, enriched with chosen key ISO standards and frameworks regulating the field. The methodology deliberately combined exactly these particular standards and frameworks with insights from ENISA and recent threat intelligence to create a coherent and operational tool.

The purpose of the model is to connect legal duties with operations by integrating cyber, physical, and AI risk dimensions into one lifecycle, while its goal is to provide organisations with a practical yet adaptable structure for demonstrating accountability, trust, and preparedness. Its limitations are openly acknowledged: the framework still awaits empirical validation in industry, smaller operators may need scaled versions, and evolving legislation will require continuous updates. Nonetheless, its strength lies in offering a structured pathway that connects governance to operational practice, compliance to resilience, and security to long-term integrity.

From the authors' experience in both research and direct engagement with operators – the biggest risk is not the absence of frameworks but the mismatch between what is written in policies and what happens in practice. Media coverage and even some academic papers often simplify incidents, which can (unintentionally) cause more harm to organisations already under attack by distorting public perception and regulatory pressure.

In conclusion, resilience in the 21st century cannot be achieved by firewalls or policies alone. It requires resilience-by-design and security-by-design principles embedded from the start, supply chains governed with transparency and trust and AI risks managed as integral components of systemic security. By applying the proposed model, critical infrastructure operators can move beyond reactive protection towards proactive, evidence-based resilience, capable of withstanding complex and evolving threats of a connected and obviously uncertain world.

Equally important is the recognition that *data is now a core operational asset* and that its exposure through leakage, corruption, manipulation, or unavailability can compromise not just IT systems

but public trust, systems and services continuity, and even human safety itself. When AI systems depend on this data, *the risks multiply*, making it imperative to treat data integrity and supply chain transparency as inseparable. At the end, securing critical infrastructure in the 21st century means securing what it depends on: extended digital, physical, and cognitive supply networks that make modern services possible.

To translate the model into immediate practice, operators can take one low-friction action in the coming week: require every supplier renewal or new engagement to provide (1) a software bill of materials (SBOM) or model card for AI component sand (2) a defined point of contact for 24-hour incident reporting. These two clauses alone significantly improve visibility and speed of response.

Applying this model helps organisations move from reactive protection to proactive, auditable, and adaptive resilience in dealing with everyday new physical, social, and technical threats and vulnerabilities to our critical infrastructure services and society.

Acknowledgements

To ensure clarity and consistency in English, AI-based translation tools were used for language translation and style polishing. The content, structure, and scientific contributions remain the sole work of the authors.

References

[1] European Union (EU), "NIS2 directive, 'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union'," *Official Journal of the European Union*, 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj. [Accessed: Jun. 5, 2025].

[2] European Union (EU), "CER directive, 'Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC'," *Official Journal of the European Union*, 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2557/oj. [Accessed: Jun. 5, 2025].

[3] Cybersecurity and Infrastructure Security Agency (CISA). (2020). AA20-352A: Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a. [Accessed: May 2, 2025].

[4] Symantec. (2017). :What you need to know about the Petya/NotPetya ransomware. Broadcom." [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/petya-ransomware-wiper. [Accessed: Apr. 5, 2025].

[5] A. Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history," *Wired*, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. [Accessed: May 12, 2025].

[6] Reuters. (2023). MOVEit hack spawned over 600 breaches but is not done yet -cyber analysts. [Online]. Available: https://www.reuters.com/technology/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08/. [Accessed: Aug. 20, 2025].

[7] GitGuardian. (2025). The GhostAction campaign: 3,325 Secrets stolen through compromised GitHub workflows, Blog. [Online]. Available: https://blog.gitguardian.com/ghostaction-campaign-3-325-secrets-stolen/. [Accessed: Sep. 10, 2025].

[8] Palo Alto Networks Unit. (2025). *Model namespace reuse: An AI supply-chain attack exploiting model name trust*. [Online]. Available: https://unit42.paloaltonetworks.com/model-namespace-reuse/. [Accessed: Aug. 20, 2025].

[9] Mandiant. (2023). 3CX software supply chain compromise initiated by a prior software supply chain compromise; suspected North Korean actor responsible. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise. [Accessed: Aug. 21, 2025].

[10] Akamai. (2024). XZ utils backdoor – Everything you need to know, and what you can do. [Online]. Available: https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know. [Accessed: Aug. 24, 2025].

[11] TechRadar Pro. (2025). Compromised files replace *npm* packages with a combined 2 billion weekly downloads. [Online]. Available: https://www.techradar.com/pro/security/compromised-files-replace-npm-packages-with-a-combined-2-billion-weekly-downloads. [Accessed: Aug. 25, 2025].

[12] IT Pro. (2025). Air France and KLM confirm customer data stolen in third-party breach. [Online]. Available: https://www.itpro.com/security/data-breaches/air-france-and-klm-confirm-customer-data-stolen-in-third-party-breach. [Accessed: Aug. 25, 2025].

[13] The Guardian. (2025). Qantas confirms cyber-attack exposed records of up to 6 million customers. [Online]. Available: https://www.theguardian.com/business/2025/jul/02/qantas-confirms-cyber-attack-exposes-records-of-up-to-6-million-customers. [Accessed: Aug. 28, 2025].

[14] M.G. Collu, T. Janssen-Groesbeek, S. Koffas, M. Conti, S. Picek, "Dr. Jekyll and Mr. Hyde: Two faces of LLMs," *arXiv preprint*, arXiv:2312.03853, 2023, doi: 10.48550/arXiv.2312.03853.

[15] European Union (EU), "Cyber Resilience Act, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 13 March 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020," *Official Journal of the European Union*, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj. [Accessed: Sep. 8, 2025].

[16] International Organization for Standardization. (2023). Security and resilience – Security management systems – Requirements (ISO 28000:2022). [Online]. Available: https://www.iso.org/standard/79612.html. [Accessed: Jun. 5, 2025].

[17] International Organization for Standardization. (2014). Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance (ISO 28001:2007). [Online]. Available: https://www.iso.org/standard/45654.html. [Accessed: Jun. 5, 2025].

[18] International Organization for Standardization. (2018). Risk management – Guidelines (ISO 31000:2018). [Online]. Available: https://www.iso.org/standard/65694.html. [Accessed: Jun. 5, 2025].

[19] International Organization for Standardization & International Electrotechnical Commission. (2022a). Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC 27005:2022). [Online]. Available: https://www.iso.org/standard/80585.html. [Accessed: Jun. 5, 2025].

[20] International Organization for Standardization & International Electrotechnical Commission. (2022b). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022). [Online]. Available: https://www.iso.org/standard/27001. [Accessed: Jun. 5, 2025].

[21] International Organization for Standardization & International Electrotechnical Commission. (2022c). Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022). [Online]. Available: https://www.iso.org/standard/75652.html. [Accessed: Jun. 5, 2025].

[22] International Organization for Standardization. (2024). Information technology – Artificial intelligence – Guidance on risk management (ISO/IEC 23894:2023). [Online]. Available: https://www.iso.org/standard/77304.html. [Accessed: Jun. 5, 2025].

[23] International Organization for Standardization. (2023). Information technology – Artificial intelligence – Management system (ISO/IEC 42001:2023). [Online]. Available: https://www.iso.org/standard/81230.html. [Accessed: Jun. 5, 2025].

[24] National Institute of Standards and Technology (NIST). (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). doi: 10.6028/NIST.AI.600-1.

[25] European Union Agency for Cybersecurity (ENISA). (2025). ENISA NIS360 2024: ENISA cybersecurity maturity & criticality assessment of NIS2 sectors, publication No. TP-01-25-002-EN-N. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-nis360-2024. [Accessed: Jun. 5, 2025].

[26] European Union Agency for Cybersecurity (ENISA). (2023). Good practices for supply chain cybersecurity, publication No. TP-03-23-145-EN-N. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity. [Accessed: May 3, 2025].

[27] European Union Agency for Cybersecurity (ENISA). (2025). *Handbook for Cyber Stress Tests*, publication No. TP-01-25-009-EN-N. [Online]. Available: https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests. [Accessed: Jun. 6, 2025].

[28] C. Novelli, P. Hacker, J. Morley, J. Trondal, L. Floridi, "A robust governance for the AI Act: AI office, AI board, scientific panel, and national authorities,"

European Journal of Risk Regulation, vol. 16, no. 2, pp. 566–590, 2025, doi: 10.1017/err.2024.57.

[29] European Union (EU), "AI Act, 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain union legislative acts (Artificial Intelligence Act)'," *Official Journal of the European Union*, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2024/1689/oj. [Accessed: Aug. 25, 2025].

[30] H. Ruschemeier, J. Bareis. (2024). Searching for harmonised rules: Understanding the paradigms, provisions and pressing issues in the final EU AI Act, *Social Science Research Network (SSRN)*, 43 p. [Online]. Available: https://doi.org/10.2139/ssrn.4876206. [Accessed: Aug. 25, 2025].

[31] N. Mündler, J. He, S. Jenko, M. Vechev, "Self-contradictory hallucinations of large language models: Evaluation, detection and mitigation," *arXiv preprint*, arXiv:2305.15852, 2023, doi: 10.48550/arXiv.2305.15852.

[32] J. Kim, N. Yang, K. Jung, "Persona is a double-edged sword: Mitigating the negative impact of role-playing prompts in zero-shot reasoning tasks," *arXiv preprint*, arXiv:2408.08631, 2024, doi: 10.48550/arXiv.2408.08631.

[33] P. Shojaee, I. Mirzadeh, K. Alizadeh, M. Horton, S. Bengio, & M. Farajtabar, (2025). The Illusion of Thinking: Understanding the Strengths and Limitations of Reasoning Models via the Lens of Problem Complexity. SuperIntelligence - Robotics - Safety & Alignment, 2(6), doi: 10.70777/si.v2i6.15919

[34] Z. Zhang, H.A. Hamadi, E. Damiani, C.Y. Yeun, F. Taher, "Explainable artificial intelligence applications in cyber security: State-of-the-art in research," *IEEE Access*, vol. 10, pp. 93104–93139, 2022, doi: 10.1109/access.2022.3204051.

[35] European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity of AI and standardisation, publication No. TP-03-23-011-EN-C. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation. [Accessed: May 22, 2025].

[36] M. Schmitt (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection, Journal of Industrial Information Integration, Volume 36, 100520, ISSN 2452-414X, doi: 10.1016/j.jii.2023.100520.

[37] R. Laroche, R. Tachet des Combes, "Dr. Jekyll & Mr. Hyde: The strange case of off-policy policy updates," *arXiv preprint*, arXiv:2109.14727, 2021, doi: 10.48550/arXiv.2109.14727.

[38] S. Bharati, P. Podder, "Machine and deep learning for IoT security and privacy: Applications, challenges, and future directions," *Security and Communication Networks*, vol. 2022, pp. 1–41, 2022, doi: 10.1155/2022/8951961.

[39] European Union Agency for Cybersecurity (ENISA). (2023). Artificial intelligence and cybersecurity research: ENISA research and innovation brief, publication No. TP-04-22-155-EN-N. [Online]. Available: https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research. [Accessed: May 22, 2025].

[40] Y. Yigit, M. A. Ferrag, M. C. Ghanem, I. H. Sarker, L. A. Maglaras, C. Chrysoulas, N. Moradpoor, N. Tihanyi, & H. Janicke. Generative AI and LLMs for Critical

Infrastructure Protection: Evaluation Benchmarks, Agentic AI, Challenges, and Opportunities. Sensors, vol. 25, no. 6, p. 1666, 2025, doi: 10.3390/s25061666.

[41] I. Botunac, N. Parlov and J. Bosna, "Opportunities of Gen AI in the Banking Industry with regards to the AI Act, GDPR, Data Act and DORA," 2024 13th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2024, pp. 1-6, doi: 10.1109/MECO62516.2024.10577936.

[42] G. Akrap, M. Kamenetskyi, "Hybrid threats and the power of identity—Comparing Croatia and Ukraine," in *Preparing for hybrid threats to security—Collaborative preparedness and response*, O.J. Borch, T. Heier, Eds. New York, NY: Routledge, 2024, pp. 218–233, doi: 10.4324/9781032617916.

[43] G. de Valk, "Analytic black holes: A data-oriented perspective," *National Security and the Future*, vol. 23, no. 1, pp. 21–48, 2022, doi: 10.37458/nstf.23.1.1.

[44] G. Akrap, "Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura," *Strategos*, vol. 3, no. 2, pp. 37–49, 2019. [Online]. Available: https://hrcak.srce.hr/231009. [Accessed: Jun. 1, 2025].

[45] K. Meding, C. Sorge, "What constitutes a deep fake? The blurry line between legitimate processing and manipulation under the EU AI Act," in *Proceedings of 2025 Symposium on computer science and law (CSLAW '25)*. New York, NY: ACM, 2025, pp. 152–159, doi: 10.1145/3709025.3712218.

[46] CEN-CENELEC. Artificial intelligence. [Online]. Available: https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/. [Accessed: Jun. 1, 2025].

[47] J.A. Martin and C. Baccarani. (2021). AI in management: Dr. Jekyll or Mr. Hyde?, in Proceedings of the 11th European International School on Information and Communication Technologies (EISIC), University of Verona. [Online]. Available: https://sites.les.univr.it/eisic/wp-content/uploads/2021/10/27-Martin-Baccarani.pdf. [Accessed: Apr. 4, 2025].

[48] European Commission. (2025). AI Act. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. [Accessed: May 14, 2025].

[49] N. Parlov, Ž. Sičaja, T. Katulić, R. Luša, "Information security and the lawful interception of communications through telecom service providers infrastructure: Advanced model system architecture," *Policija i Sigurnost (Police and Security)*, vol. 30, no. 1, pp. 112–130, 2021.

[50] E. Glerean. (2025). Fundamentals of secure AI systems with personal data, European Data Protection Board, Support Pool of Experts Programme. [Online]. Available: https://www.edpb.europa.eu/system/files/2025-06/spe-training-on-ai-and-data-protection-technical_en.pdf. [Accessed: Jul. 3, 2025].

[51] European Union (EU), "Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and Regulation (EU) 2016/1011," *Official Journal of the European Union*, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj [Accessed: Sep. 8, 2025].

[52] European Union (EU), "Artificial Intelligence Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down

harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828," *Official Journal of the European Union*, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. [Accessed: Sep. 10, 2025].

[53] Deloitte. (2020). Understanding the value of your data assets. [Online]. Available: https://www.deloitte.com/content/dam/assets-shared/en_gb/legacy/docs/Valuation-Data-Digital.pdf. [Accessed: Aug. 19, 2025].

[54] J. Esterajher, P. Mihaljević. (2020). Manipulacija informacijama kao ugroza demokracije // Zbornik radova međunarodne znanstveno-stručne konferencije 6. Istraživački dani Visoke policijske škole u Zagrebu – „Idemo li ukorak s novim sigurnosnim izazovima?/Cajner Mraović, Irena; Kondor Langer, Mirjana (ur.). Zagreb: Ministarstvo unutarnjih poslova Republike Hrvatske, pp. 465–477. Available: https://cpi.gov.hr/UserDocsImages/konferencije/IDVPS/VII/zbornik/MUP%20zbornik%20radova%207%20-%206%20Esterajher.pdf. [Accessed: Sep. 4, 2025].