CYBERSECURITY AND AI: STRENGTHENING DIGITAL RESILIENCE IN EUROPE

Marta González Barragán

Legal Assistant at the Spanish Delegation in Brussels of Colegio de Registradores

Abstract

Europe is facing an escalating threat from cyberattacks and disinformation campaigns, targeting critical infrastructure and democratic stability. In response, it has implemented comprehensive measures such as the NIS2 Directive, the Cyber Resilience Act, and the AI Act, aiming to enhance cybersecurity and regulate emerging technologies responsibly. These initiatives underscore Europe's commitment to safeguarding fundamental rights while fostering innovation. The NIS2 Directive expands cybersecurity requirements across sectors, while the Cyber Resilience Act enforces security standards for connected devices. The AI Act, a global regulatory benchmark, addresses risks linked to artificial intelligence, promoting transparency and ethical practices. Moreover, efforts like the Cybersecurity Skills Academy emphasize digital literacy and professional capacity-building to reinforce societal resilience. By integrating legal frameworks, technological innovation, and collaborative initiatives, Europe is shaping a secure, inclusive digital ecosystem that balances progress with social responsibility, offering a model for global digital governance.

Keywords: cybersecurity, artificial intelligence, digital resilience, NIS2 Directive, AI Act

…….

In recent years, Europe has witnessed a notable surge in cyber-attacks targeting critical infrastructure, underscoring the urgent need to enhance digital resilience. Concurrently,

Europe is at the forefront of the global response, spearheading advanced regulations, fostering collaborative initiatives, and demonstrating a steadfast commitment to responsible innovation.

The increasing reliance on digital systems has heightened the vulnerability of institutions and businesses to increasingly sophisticated cyberattacks. From data manipulation to disinformation campaigns, these threats not only impact critical infrastructures but also directly affect the stability of democracies and the protection of fundamental rights.

Considering this reality, Europe has established itself as a benchmark in creating regulatory frameworks and promoting strategic alliances among governments, businesses, and citizens. These actions aim not only to mitigate the risks associated with technological advancement but also to ensure that digital progress develops ethically, inclusively, and in alignment with specific legal standards. Regulatory efforts such as the NIS2 Directive and the AI Act exemplify a comprehensive approach encompassing both prevention and response to these challenges.

Artificial intelligence, in particular, is profoundly transforming how cybersecurity is addressed. Advanced systems enable real-time threat identification, analysis of large data volumes, and attack prediction before they occur. This capability not only reinforces critical infrastructures but also enhances incident management efficiency by reducing response times and mitigating potential damage. At the same time, AI creates opportunities for process automation and skills enhancement through technologies like advanced language models, which can analyze and correlate key information to support more informed decision-making.

However, this tool is not solely at the service of defense. The same capabilities that make AI indispensable for cybersecurity are also being used by malicious actors to enhance cyberattacks. Automated tools enable massive, highly personalized phishing campaigns, while technologies like deepfakes have proven effective in spreading false content to manipulate public opinion or destabilize democratic processes.

The growing convergence between cyberattacks and disinformation presents a significant challenge for modern democracies. These threats aim not only to compromise systems

but also to erode social trust and manipulate public narratives during critical processes, such as elections. In this environment, the combination of advanced technology and psychological strategies amplifies the impact of attacks, exacerbating social divisions and creating uncertainty among populations. Thus, it is essential to implement robust technological defenses while fostering a culture of digital literacy that enables citizens to distinguish reliable information from deliberate manipulation.

Strengthening the European legal framework is a fundamental pillar in the fight against growing cyber threats and the misuse of advanced technologies. Digitalization of critical infrastructures, public services, and strategic sectors requires a regulatory environment capable of responding swiftly and effectively to emerging challenges. Europe, aware of these challenges, is working on a framework that seeks to balance technological innovation with social responsibility.

The NIS2 Directive is a key component of this regulatory ecosystem. It revises and expands the scope of the previous directive, requiring more essential sectors and digital service providers to adopt stricter cybersecurity measures. This framework not only mandates the implementation of advanced technical and organizational measures but also introduces strict incident reporting requirements to ensure a rapid and coordinated response to cyberattacks. Additionally, the directive emphasizes the importance of securing supply chains, given the rise in threats targeting partners and providers.

In parallel, the Cyber Resilience Act addresses specific risks associated with the proliferation of connected devices within the Internet of Things (IoT)[1]. This regulation imposes mandatory requirements on manufacturers, such as conducting risk assessments and implementing preventive measures before products reach the market. By mandating a security-by-design approach, Europe aims not only to protect consumers but also to foster trust in digital technologies. This framework is especially relevant in an environment where device connectivity represents both an opportunity and a significant risk.

[1] The Internet of Things (IoT) encompasses a network of everyday objects—ranging from household appliances to vehicles—integrated with sensors, software, and connectivity. This technology allows these objects to communicate, share data, and interact autonomously within digital ecosystems.

In the field of artificial intelligence, the AI Act sets a global precedent by regulating this technology through a risk-based approach. The regulation classifies AI systems into several categories, from low-risk applications to high-risk uses, such as those in critical infrastructure, judicial decisions, or hiring processes. The law explicitly prohibits practices deemed incompatible with fundamental rights, such as mass biometric surveillance in public spaces. It also requires developers to ensure algorithm traceability and auditability, promoting transparency and ethical responsibility. In this sense, the AI Act addresses technological risks while establishing a framework that fosters responsible innovation and prevents the misuse of these tools, especially in sensitive contexts like information manipulation or automated generation of misleading content.

These regulations do not operate in isolation but are part of a comprehensive approach that includes initiatives such as EuRepoC, a European repository of cyber incidents that collects data on cyber operations with political implications. This resource not only helps detect patterns and anticipate threats but also supports evidence-based policymaking to address transnational challenges.

Europe complements these regulatory efforts by promoting digital skills and cross-sector collaboration. Initiatives like the Cybersecurity Skills Academy address the shortage of cybersecurity professionals by providing specialized training and capacity-building programs tailored to current and future labour market needs.

Building effective digital resilience inevitably requires strengthening a legal framework that is both robust and adaptable. Europe has understood that in the face of global threats like cyberattacks and disinformation, law must play a central role—not only as a protective tool but also as a driver of trust in an increasingly complex digital environment.

However, the law cannot function in isolation. Its effectiveness depends on its ability to adapt to an ecosystem where technology evolves faster than ever. Therefore, integrating legal frameworks with practical initiatives, such as digital skills training and transnational cooperation, is crucial to ensuring these regulations translate into real, sustainable solutions.

Europe not only legislates to protect critical infrastructures or regulate artificial intelligence but also sets global precedents by building a legal model that recognizes the interdependence between security, rights, and progress. This approach reinforces its position in the digital realm, offering a pathway that combines technological innovation with respect for fundamental principles.

The future of digital resilience will ultimately depend on Europe's ability to continue consolidating this comprehensive legal framework. A framework that not only reacts to threats but anticipates challenges, promotes ethical technology use, and ensures that digital progress serves society as a whole.