

Cybersecurity Regulations and Software Resilience: Strengthening Awareness and Societal Stability

Roland Kelemen^{1*} – Joseph Squillace² – Ádám Medvác³ – Justice Cappella⁴

¹ Széchenyi István University, Győr, Hungary, ORCID ID: 0000-0002-5419-8425, kelemen.roland@ga.sze.hu

² Penn State University, Schuylkill Haven, United States of America, ORCID ID: 0000-0003-4227-5144, jms10943@psu.edu

³ Széchenyi István University, Győr, Hungary, ORCID ID: 0009-0007-6071-8777, adam.medvacz@gmail.com

⁴ Penn State University, Schuylkill Haven, United States of America, ORCID ID: 0009-0009-9788-9582, justicecappella@gmail.com

*Corresponding Author

Abstract: The aim of this study is to explore how cybersecurity regulation focused specifically on software security can shape societal resilience—particularly in light of progress toward the Sustainable Development Goals (SDGs 5, 10, and 16). The research follows four analytical strands: qualitative interpretation of EU and US strategic documents, comparative legal analysis, case-based evaluation of the software development life cycle (SDLC), and a normative-sociological reading grounded in discourse analysis. The findings indicate that the selected regulatory instruments—most notably the EU’s Cyber Resilience Act and NIS2 Directive, as well as the United States’ 2023 Cybersecurity Strategy and SBOM requirements—are not mere reactions to emerging threats. They function as structural mechanisms that embed resilience as a normative operating principle. Software security emerges as a field where trust is redistributed and institutional responsibility is renegotiated: through the reallocation of digital risks between developers, vendors, and users, cybersecurity is reframed not only as technical compliance but as a matter of social justice. The study shows that when consistently applied, the “resilience-by-design” approach enables regulatory frameworks to integrate democratic participation, digital equity, and the protection of vulnerable populations as systemic objectives. This approach links technological development with social cohesion—not only as parallel goals, but as elements of a shared regulatory logic.

Keywords: software security regulation, societal resilience, resilience-by-design, cybersecurity governance, sustainable development goals

1. Introduction

A seemingly isolated disruption can set off a chain reaction – destabilizing institutions, disrupting the flow of essential services, and slowly unraveling the fabric of public trust that modern societies depend upon. The World Economic Forum’s 2023 Global Risks Report makes this point unmistakably clear: ransomware campaigns and software supply chain attacks are no longer confined to corporate networks. They have crossed over into public life – posing risks to economic stability, infrastructure, and the very capacity of societies to absorb shocks and stay functional. These incidents are not isolated anomalies; they form part of a pattern. And this pattern increasingly blurs the line between cybersecurity and public resilience. When digital infrastructures fail, as seen in the 2016 Bangladesh Bank breach (Brewster, 2016) or the 2021 Colonial Pipeline incident (Easterly & Fanning, 2023), what breaks down is not merely a system – but trust. When trust erodes, its consequences are rarely confined to institutional dysfunction – in some cases, the rupture rises to the level of national security.

In this context, cyber resilience can no longer be reduced to a technical posture. It is increasingly understood as the technological extension of a deeper societal capacity – one that depends not only on resistance, but on the ability to recover, adapt, and reorganize. These days, when we talk about resilience, we’re no longer just talking about systems that hold the line. What we mean – what we increasingly have to mean – is something deeper. Something that moves with the disruption, absorbs it, learns from it, and keeps going. That’s why concepts like “resilience-by-design” or “zero trust” have started showing up not just in engineering manuals,

but in policy papers (Van Bossuyt et. al., 2023). They've crossed over. They're now part of how we think about trust – about how institutions endure, how people stay included, and how legitimacy is built when systems are tested. It's not just about fending off attacks anymore. It's about keeping the core structure of public life from coming apart.

Within this shifting terrain, the meaning of resilience itself is changing. It is no longer a score on a readiness index, but a normative structure – a way of organizing technical, legal, and social decisions so that digital infrastructures don't just work but hold together under pressure. This shift is perhaps nowhere more visible than in how we've come to see software security – not just as a coding problem, but as a political one. A social one. The most damaging attacks aren't the loudest. They're the ones that slip through cracks we've left open – unpatched systems, unclear ownership, update chains no one really tracks. And while new technologies like SOAR or AI-driven detection are changing the game, they don't work in a vacuum. Without legal clarity, without norms to anchor them, even the best systems fall short. Resilience needs more than code. It needs structure. And trust.

This study begins from a simple premise: we cannot understand societal resilience without examining how cybersecurity regulation is structured. It is not enough to ask what technical safeguards exist – we must ask how they are framed in law, how they allocate responsibility, and how they contribute to broader policy goals, especially the Sustainable Development Goals (SDGs 5, 10, and 16). From this perspective, the central question of the paper becomes clear: do the cybersecurity regulations of the EU and the US – particularly those dealing with software – merely react to threats, or can they offer structural responses to the vulnerabilities of digital society? Can they help not only to defend, but to build?

2. Literature Review

In the context of social resilience, we refer to those capacities through which individuals, micro- or macro-level communities, or society as a whole are able to respond effectively to disruptions of ordinary processes (Cañizares et al., 2021). The relationship between cybersecurity and social resilience is particularly close. It is worth approaching the academic literature from a policy perspective. This convergence between the two fields was already highlighted in the European Union's 2013 Cybersecurity Strategy, which emphasized the need to strengthen individual cybersecurity awareness, and among other measures, introduced the European Cybersecurity Month. NATO, for its part, by recognizing cyberspace as a domain equivalent to traditional theatres of war, initially focused on building the resilience of its personnel. However, in the wake of the hybrid war in Ukraine and the growing number of cyberattacks from China, Russia, and North Korea, the 2018 Brussels Summit Declaration went further and committed itself to developing a comprehensive, multi-layered form of cyber resilience covering society as a whole (Brussels Summit Declaration, 2018).

In the following decade, documents from both organizations have consistently emphasized the importance of societal adaptability to the cyber domain as a core element of resilience. The EU's 2017 and 2020 Cybersecurity Strategies already describe cyberattacks as national security threats, and underline that strengthening social resilience in this area is among the key conditions of an effective response. The urgency of this need was only intensified by the COVID-19 pandemic and the subsequent outbreak of war in Ukraine (Kuzior et al., 2024; Farkas & Vikman, 2024; Kelemen, 2023). NATO's 2021 declaration, the Strengthened Resilience Commitment, described national and collective resilience as guarantees of credible deterrence. Within the NATO 2030 framework, improving social resilience – specifically in the area of cybersecurity – was set as a priority, a goal further reinforced in the 2022 NATO Strategic Concept, which ties this to the imperative of maintaining technological superiority.

Academic discourse has likewise begun to explore the nexus between cybersecurity and social resilience. Arturo Escobar was among the first to argue that technology is not separate from the social world – it is shaped by it, and in turn influences it. In his view, the kinds of tensions we see in physical space also appear in cyberspace, which means resilience strategies need to account for these dynamics too (Escobar, 1994). This perspective later gave rise to the idea of socio-technical vulnerability, which holds that cybersecurity and cyber resilience are influenced not just by technical factors, but also by people's lived experiences and the values embedded in society. Accordingly, cybersecurity should be understood as a combination of social problem plus technology, rather than a purely technical problem involving human operators (Cavelty et al., 2023).

A particularly relevant approach in this context is that of resilience-by-design. The idea of embedding resilience into system design is gaining ground. As Colabianchi and colleagues point out, systems that take resilience into account from the outset are better equipped to withstand disruption and adapt to change. In practice, this means designing cyber infrastructures that are not only technically sound but also built with an awareness of their social environment. By embedding resilience from the outset – rather than treating it as an add-on – these systems can remain functional even when conditions turn unpredictable or hostile. This forward-looking approach is especially important in today's vulnerable and rapidly shifting digital ecosystems (Colabianchi et al., 2021).

Recent contributions also highlight the need to better understand cyber threats at the individual level, as this awareness is often the first step toward preventing systemic failures. Several authors have pointed out that the increasing complexity of cyber threats requires more than ad hoc responses. A structured, multi-level preparedness model has therefore been proposed, allowing institutions to react to evolving risks in a more deliberate and adaptive manner (Saeed et al., 2023). In parallel, national cybersecurity strategies have gained recognition not only as technical frameworks, but also as key policy instruments that shape public awareness and contribute directly to strengthening social resilience (Aldaajeh et al., 2022). It is also a recurring theme that mitigating cyber threats requires the development of advanced digital skills (Kelemen et al., 2024). Initiatives in education that aim to foster these competences are therefore of central importance to the qualitative improvement of social resilience (Maurer & Fritzsche, 2023).

The socio-technical model and the resilience-by-design principle are also relevant in the field of software development (Colabianchi et al., 2021). Embedding cybersecurity into development workflows is no longer optional – it's become a core element of responsible digital design. This is evident in how agile methodologies are now combined with continuous iteration and testing, while secure design principles are embedded across the full software lifecycle. Add to this the implementation of resilient interfaces – such as multi-factor authentication – and the result is a significant step toward building digital tools that are both secure and sustainable (Tashtoush et al., 2022; Andrade et al., 2023; Von Solms & Fitcher, 2020). At the same time, the human factor remains equally important – both in terms of responsible software development and conscious use. On the developer side, this means intentionally incorporating cybersecurity requirements into programming; on the user side, it includes making informed choices about software and applying updates regularly (Gasiba et al., 2020; Xiao & Spanjol, 2021; Sun et al., 2024). Taken together, these factors enhance both cybersecurity resilience and social resilience in qualitative terms.

The literature also points to the fact that social resilience, cybersecurity, and software development have implications for achieving the Sustainable Development Goals (SDGs). These connections can be direct or indirect: cybersecurity is now essential in the context of SDG 4C (quality education), SDG 9 (industry, innovation and infrastructure), and SDG 9C (access to digital technologies), which is a prerequisite for improving cyber resilience. In

addition, the strengthening of cybersecurity resilience may also contribute to SDG 16, which aims to promote peaceful, just and inclusive societies – since more robust defence mechanisms can reduce the effectiveness of cyberattacks and thereby help diminish cybercrime and organized criminal activity (Dede et al., 2024; Aziz et al., 2025; Popkova et al., 2022).

From the above, it is clear that both NATO and the European Union treat cybersecurity as a top priority, and at present, as a core pillar of social resilience. Most of the literature agrees that cybersecurity should not be reduced to a technical issue alone. Its social aspects are equally critical, often shaping the very conditions under which resilience can emerge. This recognition also brings certain responsibilities at the level of public policy. Efforts to increase awareness, rethink education, and support secure development and use of software are not peripheral – they form the backbone of any serious attempt to build social resilience. The literature also indicates that these efforts are closely aligned with the broader objectives of the SDGs. Building on the theoretical and empirical interconnections highlighted in existing research, this study aims to draw attention to an aspect that has received relatively little attention so far: namely, whether and how cybersecurity regulation – particularly in the field of software – can serve as a tool through which lawmakers intend to shape social resilience. While the societal significance of cybersecurity has been confirmed at multiple levels in the literature, this paper examines the extent to which legal instruments aim to contribute explicitly to strengthening social resilience.

3. Methodology

This study sets out to explore how cybersecurity regulation – particularly in the field of software security – can shape not only the technical contours of protection but also the social architecture of resilience. The approach is deliberately interdisciplinary, weaving together the interpretive depth of legal theory, the structural insights of public policy analysis, the reflexivity of social thought, and the operational understanding of cybersecurity as practice. At its core lies the recognition that societal resilience cannot be reduced to technological robustness or institutional design alone. It must be approached as a contingent and multi-layered phenomenon – one that emerges at the intersection of regulatory logic, digital infrastructure, and the conditions of civic participation. The core research question guiding this study is: how do EU and US cybersecurity regulations, particularly those addressing software security, embed and operationalize the concept of societal resilience?

To address the research question comprehensively, the study mobilizes four interrelated analytical strands. Each of these targets a specific dimension of the problem: the discursive construction of resilience (1), the legal-normative embedding of security obligations (2), the technical-operational dynamics of software vulnerabilities (3), and the socio-theoretical implications of inclusive digital governance (4). The analysis rests on four core methodological approaches. The first involves a close qualitative reading of three strategic documents: the European Union’s 2020 Cybersecurity Strategy, the 2025 Internal Security Strategy (ProtectEU), and the United States’ 2023 National Cybersecurity Strategy. Rather than treating these texts as neutral policy instruments, the study applies a thematic coding-based qualitative content analysis. It systematically identifies how key terms such as “resilience,” “security by design,” and “public trust” are deployed – both in terms of semantic frequency and their positioning within the documents’ institutional, civic, and technological framing. The goal is not only to identify where and how societal resilience appears in the cybersecurity discourse, but to understand the role it plays – explicitly or by implication – in shaping regulatory priorities and aligning them with the broader ambitions of the Sustainable Development Goals, especially SDGs 5, 10, and 16. These three documents were selected due to their strategic significance in shaping cybersecurity governance at supranational (EU) and federal (US) levels following

2020, particularly in connection to regulatory responses to hybrid threats and infrastructure-level digital risks.

The second strand of the analysis applies a comparative legal method to selected regulatory texts from both the European Union and the United States – most notably the Cybersecurity Act, the Cyber Resilience Act, Executive Order 14028, the 2023 U.S. National Cybersecurity Strategy, FISMA, and provisions related to SBOM implementation. The aim is not to highlight formal legal divergences, but to examine how the concept of resilience is embedded within these frameworks: what kinds of social mechanisms they mobilize, how responsibility is distributed, and what regulatory logics underpin the public governance of technical risk. Special attention is paid to whether software security is addressed not only as a technical issue, but also as a socio-economic one: whether responsibility is extended to producers, whether transparency is mandated toward users, and whether these instruments lay the groundwork for equitable access to digital safety as a matter of public interest. The selected legal instruments represent key reference points in the evolving cybersecurity regulation landscape on both sides of the Atlantic, each offering a distinct model for how software security is governed and linked to broader societal concerns.

The third analytical strand approaches the issue from the perspective of information security and software engineering, with a particular focus on the resilience-conscious design and governance of the Software Development Life Cycle (SDLC). This section adopts a case study-based methodology, drawing on the Log4Shell vulnerability and the Equifax data breach to explore how the treatment of technical vulnerabilities becomes a matter of institutional trust and public accountability. The SDLC's four phases – introduction, growth, maturity, and decline – are interpreted not only as stages in a technical process but as points of intersection between software integrity and broader societal risk governance. The chosen case studies illuminate how failures in software security cascade across technical, institutional, and societal layers – demonstrating that resilience must be architected as a distributed property across each phase of the digital lifecycle. The methodological toolkit includes threat modelling, lifecycle-integrated security analysis, and qualitative examination of patch management and update practices. To preserve methodological consistency, this strand builds a conceptual bridge between technical vulnerability management and the normative requirements of institutional accountability, aligning the operational logic of SDLC with the social functions of trust and digital legitimacy. This approach allows SDLC to be reframed not merely as an engineering logic but as a normative and institutional arena where resilience is operationalized and maintained.

The fourth strand develops a normative-sociological interpretation of societal resilience, grounded in the conceptual frameworks of the “social-technological model” and “resilience-by-design.” Rather than measuring resilience in empirical terms, this analysis employs methods drawn from institutional hermeneutics and critical discourse analysis. Its aim is to demonstrate that resilience is not a passive condition derived from system stability, but an active capacity rooted in how citizens engage with the design, governance, and institutional framing of digital infrastructures. The analysis focuses on how regulatory expectations, institutional architectures, and cultural norms interact to shape the lived experience of digital participation. In this context, resilience emerges not as a quantifiable output but as a socially configured practice – one that manifests in structured participation, institutionalized trust, and a form of inclusion that operates as an internal logic of digital governance rather than a symbolic commitment.

At every stage, the research seeks to foster a genuine dialogue between disciplines. By integrating public policy analysis, digital legal studies, technology theory, and software engineering, the study aims to make social resilience not only a normative goal but an operational regulatory framework. The central focus is therefore not the pursuit of security for

its own sake, but its transformative potential – particularly in terms of democratic participation, digital equity, and institutional trust.

The study does not aim to measure resilience quantitatively or assess regulatory effectiveness in statistical terms. Rather, it offers an interpretive exploration of how legal and policy frameworks embed normative expectations around societal resilience.

4. Results and Discussion

4.1. The relationship between software and cybersecurity as a cornerstone of digital resilience

The advance of information and communication technologies is not simply reshaping daily life – it is reprogramming its logic. What appears as innovation on the surface carries, almost by necessity, a deepening exposure beneath it: cyberattacks are no longer erratic, but systematic, tracking the same arc as the infrastructures they target. Security, in this light, is no longer a technical supplement – it is a structural precondition for resilience. A core component of this challenge lies in software security, where – acknowledging that cybersecurity is inherently a socio-technical problem (Cavelty et al., 2023) – a key distinction must be made in terms of source code accessibility: closed (proprietary) and open-source (OSS) models follow differing development philosophies, security implications, and risk profiles, each of which has both technical and societal dimensions.

What we call source code is essentially a sequence of instructions written in a form humans can read and work with – before it's compiled into an executable application. In proprietary systems, this code remains under the control of the developer, and user access is tightly regulated through licensing agreements. Security, in this setup, rests almost entirely with the vendor – think of major actors like Microsoft or Apple – who may invest substantial resources in internal protocols, embedded protections, and regular updates. While the closed nature of the codebase can offer some protection against direct exploitation, it comes at a cost: limited transparency and a degree of vendor dependency that may, in itself, weaken resilience (Guo et. al., 2022).

Open-source models (Hadi et. al., 2024) move in a different direction. Here, the code is public by design. Projects like Linux or Apache are maintained in the open, often on platforms such as GitHub, where developers can inspect, suggest, and modify collaboratively. The idea is that public scrutiny accelerates error detection – what's sometimes called the “many eyes” effect. But openness is not the same as safety. What helps the community also helps attackers. Unlike centralized systems, open-source projects offer no single standard: updates may be irregular, documentation uneven, and code review contingent on time, trust, or the sheer availability of contributors. The model is powerful – but uneven. This community-based model, in theory, supports faster identification of vulnerabilities through what is often referred to as the “many eyes” principle. However, this model is not without risk: public access to the code allows malicious actors the same visibility as legitimate contributors; quality control and security audits are not consistently applied; and project support, documentation, and update frequency can vary significantly (Shan et. al., 2022). The Log4Shell vulnerability was never just a software bug. It functioned, rather, as a stark signal – a clear indication that even the smallest, barely perceptible fault line can trigger shockwaves capable of destabilising entire systems, institutional structures, or even the infrastructural backbone of public services. What unfolded was not simply a lapse in technical oversight, but a wider systemic warning: digital trust is not sustained by scattered, improvised patches. It rests on the regularity, coordination, and shared accountability of maintenance practices – embedded not as a technical afterthought, but as a

structural principle. And this trust cannot be upheld through isolated, improvised fixes. The lesson is clear – software maintenance cannot be an ad hoc undertaking; it must follow a deliberate and coordinated strategy. It must be sustained through regular, coordinated, and collectively embedded practices (Pigola & Meirelles, 2024). Review and maintenance are not just technical obligations. They are social contracts.

Ensuring software security and identifying its weak spots isn't a matter of picking the "right" tool. It's a matter of approach. Code review, when done properly – line by line or through automated checks – is about more than hunting for bugs; it's about making sure that fragile parts don't go unnoticed. Network sniffing is a different kind of method: it doesn't intervene, it listens. It traces the way information flows across systems, catching what was never meant to be seen. What slips through the cracks isn't always what's hidden – it's what's assumed to be safe. Penetration testing takes a more active stance: it replicates real attack scenarios in order to uncover exploitable gaps in a system's defense mechanisms. These methods, while effective on their own, become substantially more powerful when embedded throughout the entire System Development Life Cycle (SDLC) – from the earliest design stages to ongoing maintenance – supporting a proactive mindset where resilience is not an afterthought, but a structural principle (Wang et. al., 2023).

Effectively managing software security goes beyond the question of source code accessibility; it requires a security-conscious approach to the SDLC as a whole, one that also takes into account the broader socio-technical context. Optimal protection and resilience can only be achieved if security requirements and controls are consistently integrated from the very first development steps (security by design, in line with the "resilience-by-design" concept (Colabianchi et al., 2021)) through to the product's decommissioning. If we fail to integrate security from the start, we take on risks that are difficult to defend. Trust can break down, and the consequences will not stay confined to technical systems – they will spill over into society. Integrating security considerations from the earliest phases of development is not merely advisable, but essential: it allows for a more effective reduction of attack surfaces, accelerates and makes error correction more economical, and, crucially, helps to contain the scale of potential damage. The 2017 Equifax data breach illustrates this with particular clarity: although a timely patch had been issued to address the Apache Struts vulnerability, persistent organisational shortcomings meant that it was never implemented – ultimately compromising the personal data of hundreds of millions and inflicting severe and lasting harm on public trust and, by extension, on the broader fabric of societal resilience (Boss et. al., 2023). This case illustrates the critical importance of proactive vulnerability and patch management even in the later phases of the SDLC – not merely as a technical task, but as a fundamental element of system-level and societal resilience.

The concept of the SDLC is closely linked to the rapid pace of technological obsolescence in the IT sector, which necessitates not only ongoing technical adaptation of software products but also the continuous cultivation of resilience – both social and technical – and the deliberate management of the entire life cycle. The main phases of the SDLC (Khan et. al. 2022), and their specific relevance to security, particularly in light of socio-technical vulnerabilities, can be outlined as follows:

Introduction: The product is launched. At this early stage, it is critical to apply "security by design" and the broader principles of "resilience by design" in a consistent way. This includes clearly defined security requirements, initial threat modelling that accounts for both technical and user-level risks, and the establishment of secure coding practices and internal protocols.

Growth: As the user base and market visibility expand, so does the system's complexity and potential attack surface. Ongoing and increasingly in-depth security testing (e.g. penetration tests) is needed, along with timely and effective patch management processes to address

emerging vulnerabilities. At this point, socio-technical interaction becomes evident: the success of updates depends not only on the vendor but also on user awareness and cooperation.

Maturity: In the case of software, this phase is typically the longest in duration, where operational stability becomes the most expected outcome – a result of the accumulated experience of developers and the gradual increase in system complexity. Over time, the emphasis naturally shifts from functional expansion toward strategic maintenance. The regular application of updates and the timely execution of patches evolve into embedded instruments of risk management. At this point, vulnerability management must operate pre-emptively, with particular sensitivity to latent weaknesses that may only surface through extended, real-world deployment. End-user interaction and longitudinal usage data serve not merely as feedback, but as diagnostic instruments – offering critical insight into those socio-technical fault lines that standard testing regimes fail to expose.

Decline: As maintenance cycles taper off and formal support is withdrawn, the system enters a qualitatively distinct phase of exposure – one in which risk is no longer hypothetical but structurally embedded. Continuing to rely on ageing systems that no longer receive security updates embeds vulnerability not at the margins, but into the core of operations. These so-called legacy environments aren't just old – they're systems shaped by years of unresolved flaws and organisational inertia that quietly resists change. The problem isn't that they fail; it's that they continue to function while silently expanding the surface of exposure. Even in critical environments, functionality is no guarantee of stability. Systems can remain operational while quietly eroding their own margins of safety. Resilience, in this context, is not defined by continuity, but by how well a structure absorbs impact when that continuity breaks. It's not failure itself that defines the threshold – but what the failure exposes.

Security within the SDLC cannot be meaningfully addressed without considering the nature of actual cyber threats. Malware, phishing – especially the latter, which targets not the code but the user – make clear that what is exposed is not just technical surface, but human structure. DDoS attacks, ransomware, zero-day exploits: none of these test defences alone. What they reveal is whether security has been understood as a continuous process – one in which human conduct, not just system design, is accounted for from the start.

Structured and secure development processes are underpinned by international standards such as ISO/IEC 27001, offering not merely procedural guidance but a broader framework for governing information security in a dynamic environment (Kang & Kim, 2022). In parallel, modern development practices – DevOps and its security-centric extension, DevSecOps – seek to embed security, and more fundamentally resilience, into every layer of the development lifecycle. These agile and recursive approaches, grounded in testing that doesn't just verify but interrogates, and feedback that isn't a formality but a condition for movement, point less to a clean destination than to a continuous negotiation with disruption (Alghawli & Radivilova, 2024). This is where the idea of “resilience by design” becomes more than theory: not a static benchmark to be reached, but a working logic under pressure – exactly as Colabianchi et al. (2021) suggest. They operationalise the ethos of “security by design” through automated controls and support the emergence of a security-conscious development culture – one that recognises socio-technical vulnerabilities not as anomalies, but as inherent features of digital systems.

Neither the proprietary nor the open-source model offers a standalone guarantee of cybersecurity. Each has its own structural strengths and inherent limitations. What matters is not the model itself, but the discipline with which risks are managed across the software lifecycle – through testing, auditing, lifecycle-integrated controls, adherence to international standards, timely patch management, and the adoption of development and operations methods that treat security as a continuous concern rather than a final checkpoint.

4.2. From Compliance to Shared Responsibility: U.S. Cybersecurity Regulation in a Resilience Framework

Long before the 2023 cybersecurity strategy appeared in print, its outlines were already present in earlier laws, executive orders, and the silent adjustments of federal practice. Regulatory efforts were in motion, quietly but deliberately redrawing the lines around critical infrastructure and its increasingly fragile digital underpinnings. In the U.S. context, software security had already begun to outgrow its technical framing – it was becoming something else entirely: a structural condition for economic continuity, and more subtly, for public trust.

Federal procurement was suddenly contingent on the integration of security-by-design features. In practice, this had an especially strong impact in the healthcare sector, where devices like patient monitors, ventilators, and medical sensors are now subject to a higher bar of trust and protection. Earlier groundwork had already been laid by the Federal Information Security Modernization Act (FISMA) of 2014, which called on federal agencies and their contractors to develop robust cybersecurity frameworks, again with guidance from NIST. At first, it looked like a technical issue. Something for the IT teams to patch, monitor, maybe log for later. But over time, the scale changed. What was once buried in backend protocols began showing up in front-page headlines. Gradually, it stopped being about technology – and started being about strategy.

The break came in May 2021, when Executive Order 14028 hit the table. Triggered by a high-profile supply chain attack, the message was clear: the system had too many blind spots. The order didn't just tighten procurement rules – it called the bluff. Who wrote the software? Who signed off on it? Who updates it, and who disappears when it fails? Traceability wasn't a best practice anymore. It was a precondition. But more importantly, it acknowledged something that had long been avoided: that the state cannot secure its digital ecosystem without private sector alignment. Security, from that point on, was no longer a siloed duty. It had to become a shared architecture. Trust in the digital infrastructure, the order suggested, must be both shared and demonstrable.

One tangible result of this order was the launch of a cybersecurity labeling program, aimed at helping consumers make informed decisions about the software and IoT devices they purchase. Modeled after appliance energy labels, the idea was simple: before buying a device, users should know how long it will be supported, how often it's updated, and whether it meets essential security criteria. These labels were designed to be visible, understandable, and accessible – both physically and digitally.

This regulatory framework was later reinforced by a 2021 National Security Memorandum on the cybersecurity of industrial control systems managing critical infrastructure. This was the moment when the state openly conceded what had long been implicit: that it no longer holds the monopoly on securing the nation's most vital systems. From energy grids to water networks to public transport, the risks had already crossed over from speculative scenarios into tangible, measurable vulnerabilities. And in that shift, the line between public authority and private obligation began to blur – for good.

As emphasized in recent scholarship (e.g., Aldaajeh et al., 2022), national strategies and regulatory frameworks are not peripheral elements in the formation of cybersecurity awareness and community resilience; they are central drivers. Examining the regulatory and strategic environment of software security has become essential when addressing the national security significance of cyberspace. The shift in emphasis introduced by the 2023 National Cybersecurity Strategy – from the first Trump-era “forward defense” toward a cooperation-oriented model – highlights the underlying tensions between technological advancement and institutional governance. The starting point, the Cybersecurity Framework, offers a voluntary and scalable approach for critical infrastructure and government actors, placing particular

emphasis on software design, development, and supply chain security. A defining feature of the framework is its reliance not on administrative mandates, but on best practices, such as secure-by-design development. The strategy as a whole is built around five key pillars, which serve not only as the scaffolding for task allocation, but also as the space where accountability relationships are made explicit. One of the prerequisites for a functioning digital ecosystem is a regulatory framework capable of addressing the risks that come with innovation – without stifling it. This delicate balance is precisely what recent U.S. approaches have increasingly and consciously sought to achieve.

The third pillar of the U.S. cybersecurity strategy signals a structural shift: digital risks are no longer seen as individual responsibility, but as obligations that must be borne by those with systemic impact – primarily software vendors and major data operators. For the tech industry, this introduces an unfamiliar dynamic. It's not just about adopting better practices – it's about acknowledging that insecure defaults, opaque systems, and deferred updates are not technical lapses, but public risks. The strategy doesn't stop at technical prescriptions. Yes, it calls for secure-by-design development and tighter scrutiny of third-party components. But the real move is elsewhere. It shifts the weight of failure – quietly but firmly – onto those who design the systems in the first place. Not the users. Not the victims. The market is where accountability belongs, and the strategy says as much, even if not in those exact words.

In terms of resilience, that shift matters. Because what erodes trust in digital systems isn't lack of awareness – it's the quiet normalization of risk. An IoT device left exposed. A patch never issued. A legacy system still humming in the background. None of these are individual oversights. They are structural neglects, passed off as inevitabilities. And people live with the consequences. Community strength in the digital age doesn't begin with awareness campaigns or user-side caution. It begins with limiting exposure at the source. When industrial IoT devices run on default credentials, when legacy systems remain embedded in essential services, or when patches are delayed for the sake of convenience, it is not the user who fails. It is the infrastructure that abandons them. Transparency tools like SBOM, consistent update mechanisms, and enforceable liability for vendors are not abstract goals – they are preconditions for trust.

The regulatory logic outlined above not only reframes how markets operate – it also serves, indirectly but intentionally, as a tool for advancing the Sustainable Development Goals (SDGs). Cybersecurity labeling, for instance, promotes informed technology choices and helps foster digital literacy among users, which ties directly into the goal of quality education (SDG 4.4 and 4C). The transparency of update cycles and long-term vendor support, along with baseline requirements for suppliers, contribute to the reliability of digital infrastructure and encourage innovation in the security domain – supporting the objectives of industry, innovation and resilient infrastructure (SDG 9 and 9C). Strengthened supplier accountability and regulatory feedback mechanisms – for example, consequences for non-compliance with risk mitigation protocols – can also help reduce systemic vulnerability and cybercrime. In this sense, they align with the broader goal of promoting peaceful, just and inclusive societies (SDG 16.1 and 16.6). These regulatory interventions are thus not only technical in nature – they carry social and political weight. A secure digital ecosystem is not an end in itself, but a means toward long-term societal sustainability.

It is equally important to recognize that the impact of legal instruments is not uniform across social groups or institutional environments. A metropolitan hospital's cybersecurity infrastructure and protocols bear little resemblance to the informal practices of a rural school or the limited IT resources of a municipal water utility. In each case, the demand for digital security carries a different weight. Where in-house development teams exist, compliance with federal requirements may be a matter of internal alignment; where a lone IT administrator manages a fragmented system, the same regulation can become a structural burden. Even

seemingly neutral mandates – such as update obligations or SBOM integration – impose asymmetrical costs depending on institutional scale, capacity, and access to expertise. And these differences directly affect how resilience can be realized in practice.

This is why the true center of gravity for building resilience lies not in centralized distribution, but in decentralized adaptability. Schools, hospitals, local governments, civil hubs – they can only respond effectively to cyber threats when their tools, skills, and regulatory templates are allowed to connect organically. In such settings, security is not a static condition but a mode of operation defined by trust relations, accessibility, and the internal balance of adaptation. A regulation that demands rigid, one-size-fits-all compliance risks reinforcing vulnerability, rather than alleviating it. Resilience doesn't unfold from central blueprints – it takes shape in places where the rules can bend just enough to fit the people. If regulation doesn't leave room for difference, it won't hold where support is thin. And then it fails where it's needed most.

From this perspective, the third pillar of the U.S. cybersecurity strategy – centered on the redistribution of responsibility – can be seen as a practical enactment of the resilience-by-design principle. Requirements for secure software development, mandatory SBOM use, and greater supply chain transparency are not defensive measures added post hoc; they are built into the architecture from the design stage onward. In this framework, protection isn't layered on from the outside – it's embedded in how the system is supposed to work in the first place. The logic here follows what the socio-technical model has long suggested: security isn't just about shielding the technical layer. It's about building environments where the technical, the human, and the institutional are designed to support one another. That shift matters. It's what allows someone without advanced digital skills to still interact with a system safely. And that's not a small thing. It's where regulation begins to touch everyday experience – and where the digital divide, however persistent, becomes just a bit less steep. Security and social adaptability are not separate ambitions – they are part of the same operational architecture.

What emerges here is not a technocratic strategy, but a redistributive one. Risk should return to where power resides. That logic – the relocation of digital burdens from vulnerable users to dominant producers – is what ties cybersecurity policy to broader questions of societal resilience. Not every country has the leverage to do this. But for those that do, the message is clear: resilience is not stoicism. It is design.

4.3. Cybersecurity as Infrastructure: Embedding Societal Resilience through Software Regulation

Since the 2020s, the concept of societal resilience has been gaining prominence in the European Union's security and regulatory discourse. The link between cybersecurity and democratic governance no longer reflects merely a new policy perspective – it signals a deeper paradigm shift. The security of the digital environment can no longer be addressed solely as a technological or national security challenge. Instead, access to safe digital spaces, the digital competencies and participatory capacities of citizens, and the governance of platform-based threats collectively strengthen the broader resilience of society – not only in technical terms, but politically and culturally as well. This approach also reflects a social-technological model of governance, in which technical regulation and societal inclusion are treated as mutually reinforcing components of public resilience. At the same time, these measures serve multiple Sustainable Development Goals, particularly SDG 5 (Gender Equality), SDG 10 (Reduced Inequalities), and SDG 16 (Peace, Justice, and Strong Institutions).

The EU's 2020 Cybersecurity Strategy explicitly identifies digital security as a cornerstone of societal resilience. What makes the document novel is its reframing of cybersecurity – not simply as a technological or security policy issue, but as one intimately linked with fundamental

rights, the functioning of democratic institutions, and the social preconditions of both the green and digital transitions. One of its recurring conceptual anchors is “resilience,” which it interprets not merely as systemic resistance but – albeit indirectly – as a function of civic engagement, public awareness, and educational access.

Significantly, the strategy promotes the principle of “security by design” not only for critical infrastructure and services but also for the planning of digital tools, workplaces, and platforms – framing this as a technological precondition of social resilience. Secure software isn’t just a technical matter – it’s a question of who we trust to shape the systems we live by. By placing responsibility for security and vulnerability management on developers and manufacturers, the strategy draws a direct line between code and constitutional values. It suggests that public trust doesn’t begin in the courtroom or the ballot box, but in the reliability of the digital tools people use every day. In that sense, safe digital environments and everyday cyber hygiene aren’t peripheral – they are what make participation possible, what hold cohesion together.

The strategy leaves no doubt: cybersecurity is not an isolated goal – it is a foundational condition for sustainable development and for preserving what the EU holds as its core values – freedom, democracy, and the rule of law. But the path to this realization is not paved with firewalls and compliance checklists alone. The fight against disinformation, the response to hybrid threats, the investment in digital literacy, and the specific protection of women and children are not simply discrete policy fields – they are the contour lines of a broader political ambition. What emerges is the image of a society that is not only digitally equipped but socially grounded and civically responsive – a European digital citizenship, by design. It is in this context that the alignment with the Sustainable Development Goals becomes more than symbolic: SDG 5 and SDG 16 are not footnotes to this project – they are intrinsic to its architecture. A secure and inclusive digital space is not merely desirable; it is prerequisite to both gender equality and democratic coexistence.

The 2025 Internal Security Strategy (ProtectEU) carries this logic forward – sharpening it, expanding it, and embedding it more deeply into the EU’s institutional reflexes. The document’s starting point is unambiguous: cybersecurity is not just a technical terrain, but one of the structural foundations of social resilience. The proposed responses are layered – legal, technological, and civic – mirroring the hybrid nature of the threats themselves. Software security, in particular, emerges in the strategy not simply as a technical parameter, but as a structural fault line that traverses the digital infrastructure at large. What’s really at stake here isn’t just whether the code is strong – it’s whether the systems we rely on every day can be trusted to hold. In that sense, the move toward mandatory development protocols and certification isn’t just a matter of tightening the rules. It’s a way of asking: who bears responsibility when things fail? And how do we build systems that don’t just function, but deserve our trust? This is where the NIS2 Directive and the Cyber Resilience Act begin to matter – not as distant regulatory scaffolding, but as part of the blueprint itself. These are not just limits imposed from the outside; they shape the very grammar of digital design, deciding how trust is built, how responsibility is shared, and how systems remain stable when tested. They don’t just demand safety – they require it to be premeditated, engineered, lived. Alongside them, the Digital Services Act draws platform governance out of the realm of private discretion and into the domain of public accountability. Safety, in this view, is no longer a question of best intentions – it is a condition of democratic life, and must be treated as such.

But the document’s significance lies not only in what it regulates, but in how it reimagines resilience. Social cohesion is treated not as an abstract ideal, but as a fragile construct threatened by online radicalization, hate speech, and the erosion of shared truths. The measures proposed are not merely technical corrections or crisis-mitigation protocols. What the strategy sets in motion is a shift in posture – a turn from passive containment to structural anticipation. Digital crisis frameworks, reinforced protections for children, and new accountability mandates for

platforms are not ad hoc solutions; they are early markers of a governance model that seeks to foresee, not simply to respond. In this reframing, security becomes less a reaction to breaches than a precondition for civic continuity.

Equally crucial is the focus on skills and awareness, particularly among those least shielded from harm: children, women, and minorities. This is not incidental. It is the practical expression of the resilience-by-design principle: the idea that a society does not become resilient through firewalls alone, but through inclusive, participatory, and self-aware democratic formation. In this way, the strategy aligns not only with SDG 5 and SDG 16 but also with SDG 10 – reducing inequalities not as a by-product, but as a governing imperative. What takes shape here is a social-technological model in its truest sense: one in which cybersecurity frameworks, legal safeguards, and cultural norms are not separate logics but interdependent layers of the same democratic structure. And it is precisely this layered interdependence that allows digital resilience to become what it was always meant to be: societal.

It is worth briefly examining how the cybersecurity-related legislative acts referenced in these strategies – particularly those concerning software security – contribute to the objectives outlined above.

The Cybersecurity Act does not merely introduce a certification regime – it reframes cybersecurity as a structural element of democratic governance. By anchoring ENISA as a permanent agency with strategic and operational mandates, the regulation elevates digital security from a technical policy field to a matter of institutional continuity. What emerges is a governance model in which cybersecurity is not isolated from the broader political fabric but embedded within the architecture of public trust and social resilience.

The creation of a unified EU certification framework marks a subtle but significant shift. While formally voluntary, the layered logic of the Act suggests a long-term trajectory: one in which certified security becomes the normative standard, not an exception. The text places repeated emphasis on “security by design” and “security by default,” not as abstract engineering ideals, but as systemic expectations – signals to developers and manufacturers that software vulnerabilities are not merely technical oversights, but potential threats to civic stability.

Read this way, the Act speaks the language of resilience, even if it does not name it directly. It ties the reliability of digital services to the social preconditions of democratic participation. It links trust in infrastructure to the rule of law. And it aligns, however implicitly, with the aims of SDG 16: building peaceful, inclusive institutions in a digital age. In addressing the safety of essential services, the Act also resonates with SDGs 5 and 10, by setting conditions under which women, children, and marginalized users can access technology without disproportionate risk. Cybersecurity, in this frame, is no longer the shield behind the system – it becomes part of the system’s skeleton.

The Cyber Resilience Act does more than lay out technical specifications – it sketches a political vision of digital trust. By setting horizontal cybersecurity requirements for all products with digital elements, it weaves security not just into the design of devices, but into the architecture of collective resilience. The principles of “secure by design” and “secure by default” function here not as engineering preferences, but as structural conditions for maintaining societal confidence in an increasingly digital public sphere.

What ultimately gives the Cyber Resilience Act its weight is not the enumeration of technical duties, but the political clarity with which it reframes security as a long-term institutional commitment. It no longer treats digital safety as a static product feature; it defines it as an evolving responsibility embedded across the entire lifecycle of a device. The expectation is not just that manufacturers deliver something functional at launch – but that they remain answerable for the integrity of what they’ve put into circulation. Regular updates, transparent vulnerability reporting, and accountable patch management are not compliance checkboxes here; they are conditions for keeping alive the social contract on which digital trust depends.

Reporting duties, too, are reframed as instruments of collective defence. The requirement to notify both national authorities and ENISA of major incidents and exploited vulnerabilities reflects a governance logic that is no longer reactive, but anticipatory. Transparency and coordinated response are no longer virtues; they are baseline expectations of digital maturity.

The regulation's broad scope – from smart appliances to industrial control systems – ensures that its effects are not limited to niche sectors, but permeate daily life. In doing so, the CRA contributes not only to cybersecurity in a narrow sense, but to digital equity: ensuring that safe access to technology is not a privilege, but a right. This aligns with the EU's wider commitments under the Sustainable Development Goals – notably SDG 5 on gender equality, SDG 10 on reducing inequalities, and SDG 16 on fostering peaceful and inclusive societies.

At the same time, the regulation's concept of resilience is also extended to the user side. The information obligations imposed on manufacturers – such as disclosing product security features, support duration, and update availability – are intended to strengthen the awareness behind user choices. In this framework, societal resilience does not mean shielding end-users as passive recipients of protection, but enabling their active and informed participation. This reinforcement of individual decision-making capacity contributes directly to the overall security of the community.

The CRA thus exemplifies a social-technological model of resilience, in which legal obligation, technical design, and civic inclusion are no longer separable domains – but interdependent elements of a common digital future.

Based on the strategies and legislative acts examined, it becomes clear that the European Union does not merely seek to defend against threats in the digital sphere – it aims to actively shape how that sphere is embedded in society. Cybersecurity – particularly the regulation of software security – is treated not only as an end in itself but, at times, as a means: a regulatory lever through which technological reliability becomes a structural precondition for social cohesion, civic participation, and institutional trust. This approach is not technocratic, but normative and inclusive: the security of the digital environment is conceptualized as a configurable component of societal resilience. The alignment with SDGs 5, 10, and 16 is not simply rhetorical – it is substantive and operational. The EU's vision of resilience is built on reducing digital inequalities, reinforcing inclusive institutions, and universalizing access to safety. What emerges, therefore, is not just a defensive framework, but a social-technological model that doubles as a tool for shaping the democratic fabric of digital society.

5. Conclusion

This study suggests that the way we regulate software security has far-reaching consequences – not only for technical compliance, but for how resilient a society can be when pressure builds. Although the EU and the U.S. rely on different legal architectures, both seem to converge on one core insight: digital safety isn't just about keeping systems running – it's about keeping civic trust intact. The instruments analyzed – particularly the Cyber Resilience Act, Cybersecurity Act, Executive Order 14028, and SBOM-related requirements – incorporate the principles of “resilience by design” and “security by design” in a structured way, thereby aligning cybersecurity regulation with the broader goals of sustainable development.

With regard to SDG 16 (Peace, Justice and Strong Institutions), the study underscores that the reliability and maintenance of digital infrastructure must be understood not only as technical specifications, but as indicators of institutional responsibility. The failure to respond adequately to software vulnerabilities – as illustrated by the Log4Shell incident or the Equifax breach – is not just a data protection lapse; it signals a breakdown in public trust. Regulation becomes meaningful when it structures not only obligations for developers, but also the rights, awareness, and agency of users.

The relevance of SDGs 5 and 10 becomes harder to ignore once we consider how unevenly digital risk is distributed. Secure environments don't emerge from infrastructure alone – they depend on whether people can actually navigate them safely. And for that, participation matters – especially for those who are least protected by default: women, children, older adults, and communities often left out of the digital fold. Resilience, in this sense, is not equivalent to technical endurance – it is its social extension: the system's ability not only to withstand disruption but to respond to it through inclusive, participatory structures.

Accordingly, the normative repositioning of software security is not simply about re-regulating the internal logic of the digital sector. It entails the design of a governance model that integrates technological and societal dimensions. This study argues that such an integrated, socio-technical model is uniquely capable of operationalizing the conditions of societal resilience through software security – not as an after-the-fact intervention, but as a built-in mode of operation.

Conflict of interest:

The authors declare no conflict of interest.

References

- Aldaajeh, S., Saleous, H., Alrabae, S., Barka, E., Breiting, F., & Choo, K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119(102754), <https://doi.org/10.1016/j.cose.2022.102754>.
- Alghawli, A., & Radivilova, T. (2024). Resilient Cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation. *Alexandria Engineering Journal*, 107, 136–149, <https://doi.org/10.1016/j.aej.2024.07.036>.
- Andrade, R., Torres, J., Ortiz-Garcés, I., Miño, J., & Almeida, L. (2023). An Exploratory Study Gathering Security Requirements for the Software Development Process. *Electronics*, 12(17), <https://doi.org/10.3390/electronics12173594>.
- Aziz, K., Daoud, A., Singh, A., & Alhusban, M. (2025). Integrating digital mapping technologies in urban development: Advancing sustainable and resilient infrastructure for SDG 9 achievement – a systematic review. *Alexandria Engineering Journal*, 116, <https://doi.org/10.1016/j.aej.2024.12.078>.
- Boss, S., Gray, J., & Janvrin, D. (2023). Be an Expert: A Critical Thinking Approach to Responding to High-Profile Cybersecurity Breaches. *Issues in Accounting Education*, 39(1), <https://doi.org/10.2308/issues-2021-094>.
- Brewster, T. (2016). Crooks Behind \$81M Bangladesh Bank Heist Linked To Sony Pictures Hackers. *Forbes* (<https://www.forbes.com/sites/thomasbrewster/2016/05/13/81m-bangladesh-bank-hackers-sony-pictures-breach/>).
- Cañizares, J., Copeland, S., & Doorn, N. (2021). Making Sense of Resilience. *Sustainability*, 13(15), <https://doi.org/10.3390/su13158538>.
- Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research*, 26(7), <https://doi.org/10.1080/13669877.2023.2208146>.
- Colabianchi, S., Costantino, F., Gravio, G., Nonino, F., & Patriarca, R. (2021). Discussing resilience in the context of cyber physical systems. *Computers & Industrial Engineering*, 160, <https://doi.org/10.1016/j.cie.2021.107534>.
- Dede, G., Petsa, A., Kavalakis, S., Serrelis, E., Evangelatos, S., Oikonomidis, I., & Kamalakis, T. (2024). Cybersecurity as a Contributor Toward Resilient Internet of Things (IoT)

- Infrastructure and Sustainable Economic Growth. *Information*, 15(12), <https://doi.org/10.3390/info15120798>.
- Easterly, J. & Fanning, T. (2023). The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. *CISA's Blog* (<https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>).
- Escobar, A. (1994). Welcome to Cyberia – Notes on the Anthropology of Cyberculture. *Current Anthropology*, 35(3), <https://doi.org/10.1086/204266>.
- Farkas, A. & Vikman, L. (2024). Information Operations as a Question of Law and Cyber Sovereignty. *ELTE Law Journal*, 13(2), <https://doi.org/10.54148/ELTELJ.2024.2.187>.
- Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2020). Sifu - a cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity*, 24(3), <https://doi.org/10.1186/s42400-020-00064-4>.
- Guo, W., Fang, Y., Huang, C., Ou, H., Lin, C., & Guo, Y. (2022). HyVulDect: A hybrid semantic vulnerability mining system based on graph neural network. *Computers & Security*, 121 (102823), <https://doi.org/10.1016/j.cose.2022.102823>.
- Hadi, H., Ahmad, N., Aziz, K., Cao, Y., & Alshara, M. (2024). Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense. *IEEE Access*, 12 (194053-194076), <https://doi.org/10.1109/ACCESS.2024.3510533>.
- Kang, S., & Kim, S. (2022). CIA-level driven secure SDLC framework for integrating security into SDLC process. *Journal of Ambient Intelligence and Humanized Computing*, 13, 4601–4624, <https://doi.org/10.1007/s12652-021-03450-z>.
- Kelemen, R. (2023). The Impact of the Russian-Ukrainian Hybrid War on the European Union's Cybersecurity Policies and Regulations. *Connections: The Quarterly Journal*, 22(2), <https://doi.org/10.11610/Connections.22.2.55>.
- Kelemen, R., Squillace, J., Németh, R. & Cappella, J. (2024). The Impact of Digital Inequality on IT Identity in the Light of Inequalities in Internet Access. *ELTE Law Journal*, 12(2) <https://doi.org/10.54148/ELTELJ.2024.2.173>.
- Khan, R., Khan, S., Akbar, M., & Alzahrani, M. (2022). Security risks of global software development life cycle: Industry practitioner's perspective. *Journal of Software: Evolution and Process*, 36(3), <https://doi.org/10.1002/smr.2521>.
- Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, 17(2), Doi:10.14254/2071-8330.2024/17-2/12.
- Maurer, F., & Fritzsche, A. (2023). Layered structures of robustness and resilience: Evidence from cybersecurity projects for critical infrastructures in Central Europe. *Strategic Change*, 32(6), <https://doi.org/10.1002/jsc.2559>.
- Pigola, A., & De Souza Meirelles, F. (2024). Unraveling trust management in cybersecurity: insights from a systematic literature review. *Information Technology and Management*, <https://doi.org/10.1007/s10799-024-00438-x>.
- Popkova, E., De Bernardi, P., Tyurina, Y., & Sergi, B. (2022). A theory of digital technology advancement to address the grand challenges of sustainable development. *Technology in Society*, 68, <https://doi.org/10.1016/j.techsoc.2021.101831>.
- Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E., & Alabbad, D. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, 23(15), <https://doi.org/10.3390/s23156666>.
- Shan, C., Gong, Y., Xiong, L., Liao, S., & Wang, Y. (2022). A Software Vulnerability Detection Method Based on Complex Network Community. *Security and Communication Networks*. 2022(1), <https://doi.org/10.1155/2022/3024731>.

- Sun, X., Jin, J., Yang, Y., & Pan, Y. (2023). Telling the "bad" to motivate your users to update: Evidence from behavioral and ERP studies. *Computers in Human Behavior*, 153, <https://doi.org/10.1016/j.chb.2023.108078>.
- Tashtoush, Y., Darweesh, D., Husari, G., Darwish, O., Darwish, Y., Issa, L., & Ashqar, H. (2022). Agile Approaches for Cybersecurity Systems, IoT and Intelligent Transportation. *IEEE Access*, 10, <https://doi.org/10.1109/ACCESS.2021.3136861>.
- Van Bossuyt, D., Hale, B., Arlitt, R., & Papakonstantinou, N. (2023). Zero-Trust for the System Design Lifecycle. *Journal of Computing Information Science in Engineering*, 23(6), <https://doi.org/10.1115/1.4062597>.
- Von Solms, S., & Fitcher, L. (2020). Adaption of a Secure Software Development Methodology for Secure Engineering Design. *IEEE Access*, 8, <https://doi.org/10.1109/ACCESS.2020.3007355>.
- Wang, Z., Wen, Y., Wang, Z., & Zhi, P. (2023). Resilience-based design optimization of engineering systems under degradation and different maintenance strategy. *Structural and Multidisciplinary Optimization*, 66(219), <https://doi.org/10.1007/s00158-023-03671-0>.
- Xiao, Y., & Spanjol, J. (2021). Yes, but not now! Why some users procrastinate in adopting digital product updates. *Journal of Business Research*, 135, <https://doi.org/10.1016/J.JBUSRES.2021.06.066>.