



Publisher

<http://jssidoi.org/esc/home>

AI READINESS FOR SUSTAINABLE DEVELOPMENT: EUROPE'S REGULATORY BURDEN AND THE GAPS IN INNOVATION AND CYBERSECURITY

Ivana Butoracová Šindleryová ¹, Lukáš Chut'ka ^{2*}, Kamil Turčan ³, Ján Machyniak ⁴

^{1,2*,3,4} Department of Political Sciences and Public Administration, Faculty of Social Sciences, University of Ss. Cyril and Methodious in Trnava, Slovakia

E-mails: ¹ivana.butoracova@ucm.sk; ^{2*}chutka1@ucm.sk (Corresponding author); ³kamilturcan39@gmail.com; ⁴jan.machniak@ucm.sk

Received 20 May 2026; accepted 11 July 2026; published 30 September 2026

Abstract. Research examines the relationships among digital maturity, artificial intelligence (AI) readiness, and cybersecurity resilience in EU member states, highlighting their collective relevance to sustainable digital development. Drawing on multiple international datasets—including the Digital Economy and Society Index (DESI), the Government AI Readiness Index, the ITU Global Cybersecurity Index, and the European Repository of Cyber Incidents (EuRepoC)—we develop a novel composite indicator, the Digital Resilience Index (DRI). The aim is to test whether higher levels of digitalisation and AI readiness are associated with stronger cybersecurity capacity, and to identify imbalances in which rapid digital growth is not matched by adequate resilience, potentially undermining the long-term sustainability of digital governance systems. Methodologically, the study employs comparative quantitative analysis, correlation techniques, and robustness checks (Spearman coefficients and bootstrap confidence intervals) to ensure the stability of the results. The findings reveal that digitally advanced countries tend to report more incidents due to stronger monitoring and transparency, but these incidents are typically less severe. They confirm that the absence of attacks does not define resilience, but rather the ability to detect, contain, and mitigate them effectively—an essential condition for sustainable, trustworthy and future-proof digital ecosystems. By introducing an integrated index and empirically demonstrating its policy relevance, the study contributes to academic debates on digital governance and sustainable development, while offering actionable insights for policymakers. Specifically, it highlights the need to embed security-by-design principles into digital transformation, strengthen GovTech reforms, and adopt AI governance frameworks that support resilient, inclusive and sustainable digital societies.

Keywords: digital resilience; public administration; cybersecurity; AI readiness; sustainability

Reference to this paper should be made as follows: Butoracová Šindleryová, I., Chut'ka, L., Turčan, K., Machyniak, J. 2026. AI readiness for sustainable development: Europe's regulatory burden and the gaps in innovation and cybersecurity. *Entrepreneurship and Sustainability Issues*, 14(1), 223-240. <https://doi.org/10.9770/p3545922549>

JEL Classifications: F59, P16, P21

1. Introduction

The accelerating digital transformation of public administration has become a central policy priority in the European Union, especially under the framework of the European Digital Strategy and the Digital Decade 2030. Digital maturity enables governments to deliver more efficient, user-centric, and data-driven services. However, this expansion of digital infrastructures simultaneously increases the attack surface and introduces systemic vulnerabilities that can threaten public trust and national security (Eom & Lee, 2022; Kamatchi & Uma, 2025; Hazdiuk et al., 2025; Mohammed et al., 2025). While many EU member states have achieved significant progress in e-government development, research shows that digitalisation alone does not automatically lead to greater security capacity. Instead, cybersecurity must evolve in parallel with institutional, technical, and human resources (Kuziemski & Misuraca, 2020; Haug, Dan & Mergel, 2024). Without such a balance, rapid

digitalisation may pose governance risks, making states more vulnerable to ransomware, supply chain disruptions, and politically motivated cyberattacks (Hozouri, Mirzaei & Effatparvar, 2025). Artificial intelligence (AI) adds further complexity to this landscape. On the one hand, AI supports anomaly detection, incident response, and predictive analytics. On the other hand, adversarial AI, model poisoning, and deepfakes introduce novel forms of attacks that challenge existing defence mechanisms (Kaur, Gabrijelčić & Klobučar, 2023; Rjoub et al., 2023). The capacity of states to use AI responsibly—captured in governance, infrastructure, and skills—thus determines whether AI strengthens resilience or amplifies vulnerabilities (Gianni, Lehtinen & Nieminen, 2022). This article addresses these challenges by analysing the interplay between digital maturity, AI readiness, and cybersecurity resilience across the 27 EU member states. It draws on multiple datasets, including the Digital Economy and Society Index (DESI), the Government AI Readiness Index (Oxford Insights, 2024), the ITU Global Cybersecurity Index (2024), and incident-level data from the European Repository of Cyber Incidents (EuRepoC, 2025). The central aim is to examine whether higher levels of digital and AI readiness are associated with stronger cybersecurity performance and resilience, and to identify countries where digitalisation is not matched by proportional security capacity. By developing and applying a novel Digital Resilience Index (DRI), this study contributes to both academic and policy debates. The findings offer practical insights for EU policymakers, highlighting the need to embed security-by-design principles into digital government initiatives, strengthen GovTech reforms, and adopt integrated AI governance frameworks to ensure that digital transformation enhances both efficiency and security (ENISA, 2023). The urgency of studying the relationship among digital maturity, AI readiness, and cybersecurity resilience stems from governments' increasing dependence on digital infrastructure. Public administrations across the EU now operate as data-driven ecosystems where digital platforms mediate service delivery, decision-making, and citizen engagement. While this shift enhances efficiency and transparency, it also generates complex risks, as cyber incidents can undermine not only service continuity but also democratic trust and national security (ENISA, 2023; Safitra, Lubis & Fakhurroja, 2023). Moreover, the integration of artificial intelligence intensifies both opportunities and vulnerabilities. AI can support more accurate threat detection and faster responses, but poorly governed AI adoption exposes public institutions to adversarial manipulation, disinformation, and ethical concerns (Kaur, Gabrijelčić & Klobučar, 2023; Taddeo, Blanchard & Thomas, 2024). Without coordinated frameworks, governments risk creating a digital–security imbalance in which rapid innovation outpaces resilience measures (Huang & Madnick, 2019). This makes resilience a central governance challenge. Understanding which EU member states manage to align digital transformation with security capacity, and which do not, provides crucial insights for policymakers. By benchmarking resilience across countries and identifying imbalances, this study provides evidence to inform the design of future EU strategies, such as Digital Europe and the AI Act, ensuring that digital innovation is implemented responsibly and sustainably (Oxford Insights, 2024; ITU, 2024; EuRepoC, 2025). Several frameworks already exist for measuring digital maturity (DESI), cybersecurity capacity (GCI), and AI readiness (Oxford Insights, 2024). However, as Jarzębowski et al. (2024) argue, these indices capture only partial aspects of resilience and often neglect the outcomes of real-world incidents. Datasets such as the European Repository of Cyber Incidents (EuRepoC, 2025) provide a corrective by documenting the actual frequency and severity of attacks. Still, they have not yet been systematically integrated into resilience benchmarking.

2. Theoretical background

The digital transformation of public administration has become one of the most significant policy priorities in the European Union under initiatives such as the Digital Decade 2030 and the European Digital Strategy. While digital maturity enables governments to provide more efficient, citizen-oriented services, it also expands the attack surface and introduces new vulnerabilities. Research shows that digitalisation by itself does not automatically lead to higher levels of security. Instead, security capacity must co-evolve with institutional, technical, and human resources to prevent unintended risks (Eom & Lee, 2022; Kuziemski & Misuraca, 2020; Ayeola, 2025).

Cyber resilience has therefore emerged as a crucial element of digital government strategies. Comparative analyses reveal that countries that rapidly digitalised without developing systematic cybersecurity frameworks became more exposed to ransomware, phishing, and supply chain attacks. The literature stresses that digital maturity alone is insufficient unless accompanied by governance and capacity-building initiatives designed to

address security and privacy challenges (Haug, Dan & Mergel, 2024; Dritsas & Trigka, 2025; Zettl-Schabath et al., 2025).

Artificial intelligence (AI) has become a double-edged sword in this context. On the one hand, AI techniques enhance anomaly detection, threat classification, and incident response. On the other hand, adversarial AI, deepfakes, and automated exploitation introduce novel forms of attacks. Recent surveys highlight the importance of explainability, fairness, and robustness in AI-enabled cybersecurity, particularly for critical infrastructures and the public sector (Capuano et al., 2022; Rjoub et al., 2023). These findings suggest that AI readiness—including infrastructure, skills, and governance—determines whether AI functions as a defensive capability or a vulnerability amplifier (Gianni, Lehtinen & Nieminen, 2022).

Governance capacity is also a decisive factor. From a dynamic capabilities perspective, governments must continuously reconfigure their technological and institutional assets to respond to evolving cyber risks. Indicators such as the GovTech Maturity Index (GTMI) capture not only digital infrastructure but also governance mechanisms, citizen engagement, and institutional coordination, all of which are critical to embedding security by design in government platforms. Empirical studies confirm that higher GovTech maturity often coincides with stronger resilience to digital risks (Gajdzik, Grabowska & Saniuk, 2021; World Bank, 2022).

Measurement frameworks such as the Digital Economy and Society Index (DESI), the Global Cybersecurity Index (GCI), the Government AI Readiness Index, and the European Repository of Cyber Incidents (EuRepoC) provide complementary insights into the interplay between digital maturity and cyber resilience. While DESI captures the level of e-government development, GCI reflects national cybersecurity capacity, and AI Readiness highlights the ability to adopt artificial intelligence responsibly. EuRepoC, by contrast, provides evidence on the actual number and intensity of cyber incidents, offering a reality check against self-reported capacity measures (Oxford Insights, 2024; ITU, 2024; EuRepoC, 2025).

Finally, the human factor remains central to cybersecurity in the public sector. Studies demonstrate that the majority of cyber incidents originate from human error, insider misuse, or credential compromise. Advanced approaches, such as user and entity behaviour analytics (UEBA), are recommended to detect anomalies and reduce insider-related risks. European agencies emphasise that security-by-design principles, combined with AI-enabled detection systems, are essential for reducing the impact of attacks, even if the frequency of incidents remains high (ENISA, 2023). The rise of digital maturity in public administration—characterised by digitised services, data-driven decision-making, and platform interoperability—has significantly enhanced service efficiency and citizen engagement, yet simultaneously expands the cybersecurity attack surface, introducing dependencies and systemic vulnerabilities. To assess digital readiness, numerous digital government maturity models (DGMMs) have been developed, though many still inadequately address citizen-centric security dimensions—only half explicitly integrate citizen considerations into maturity frameworks (Waara, 2025).

As digitalisation accelerates, governments increasingly rely on cybersecurity maturity models to evaluate and strategically enhance their security posture, with recent systematic reviews underscoring the need for models tailored to diverse sectors and organisational sizes (Brezavšček & Baggia, 2025). The integration of artificial intelligence (AI) into cybersecurity introduces dual dynamics: it enables advanced detection, threat intelligence, and automation, while simultaneously creating novel risks such as adversarial attacks, model poisoning, and explainability deficits. Emerging studies on generative AI (GenAI) reveal its capacity to manage threat detection and response autonomously, improving efficiency. Yet, it demands robust governance, human oversight, and bias mitigation to prevent unintended consequences (Nott, 2025). The proliferation of large language models (LLMs) in cybersecurity operations enhances analytical capabilities but also raises concerns about prompt injection attacks and data exfiltration, thereby complicating traditional security controls.

From a socio-technical perspective, AI in cybersecurity must be accompanied by ethical and regulatory frameworks to ensure transparency, accountability, privacy, and human oversight, especially as AI systems permeate critical public infrastructure (Kulothungan, 2025; Taddeo, Blanchard, & Thomas, 2024). The concept of a 'risk society' highlights how AI shifts the nature of cyber threats into uncertain, reflexive domains, requiring

adaptive governance frameworks that can keep pace with evolving technological landscapes (Vulpe, 2024). Moreover, cybersecurity maturity in the public sector must redefine cybersecurity as a core governance function—not merely an IT concern—by embedding it in public administration education, institutional culture, and leadership priorities. Policy and governance scholars suggest that cybersecurity capability not only protects e-government maturity but also mediates and fosters it: increased security capabilities can reduce digital trade restrictions by promoting trust and openness (Huang & Madnick, 2019). Think-tank perspectives emphasise that cybersecurity is now foundational to digital government trust, requiring strategies from the outset rather than as retrofitted elements (Public Sector Network, n.d.; Vatamanu & Tofan, 2025). At the meta-policy level, oversight delays in AI regulation, such as moratoria at the state level, pose national security risks by slowing adaptation to AI-driven cyber threats, especially in IoT and critical infrastructure. Internationally, institutions like the Centre for Security and Emerging Technology (CSET) advise that emerging technology policies must integrate security analysis, academic insight, and nonpartisan frameworks to inform governance (CSET, 2024).

To operationalise these insights, frameworks such as cybersecurity maturity models, DGMMs, and AI governance standards must converge to guide countries through phases of digital maturity, AI readiness, cybersecurity capability, and resilience (Brohi et al., 2025). Finally, reviews in cybersecurity maturity emphasise that organisations must adopt lightweight, customisable maturity models—especially tailored for public sector and small-to-medium entities—to build resilience efficiently (Brezavšček & Baggia, 2025). Most existing studies on digital government either analyse digital maturity and cybersecurity in isolation or rely on single indices that capture only partial aspects of resilience (Kuziemski & Misuraca, 2020; Haug, Dan & Mergel, 2024). However, as comparative research shows, resilience emerges from the interaction of institutional, technological, and human capacities rather than from any single dimension. For this reason, a more integrative methodological design was necessary.

The article contributes by combining multiple internationally recognised datasets—DESI, the Government AI Readiness Index (Oxford Insights, 2024), the ITU Global Cybersecurity Index (2024), and EuRepoC incident data—into a holistic comparative analysis across all 27 EU member states. Such triangulation allows us to move beyond self-reported capacity measures and assess resilience based on both structural indicators and real-world outcomes, addressing calls in the literature for multidimensional frameworks of digital governance (Waara, 2025; Brezavšček & Baggia, 2025; Aryanti, 2025).

The methodological approach is therefore appropriate because it (1) integrates multiple dimensions of digital governance, (2) responds to gaps identified in existing literature, and (3) produces actionable insights for policymakers. In line with prior calls for policy-relevant indicators (Jarzębowski et al., 2024), this study not only provides empirical correlations but also introduces a composite index to benchmark the digital–security balance across the EU.

3. Methods and Materials

Most existing research papers analyse digital maturity and cybersecurity in isolation. This article contributes by:

- 1) integrating multiple datasets (DESI, GCI, GTMI, AI readiness, EuRepoC) into a holistic analysis—something rarely done systematically across all EU countries;
- 2) developing a novel composite indicator (Digital Resilience Index – DRI) that measures not only maturity but also resilience outcomes (using incident intensity as a corrective factor);
- 3) highlighting insider threats as an underexplored vulnerability in digital public administration and proposing a behavioural detection model combining algorithmic monitoring with policy interventions;
- 4) offering practical insights for EU policymakers: identifying states with digital–security imbalances and recommending targeted resilience-building strategies.

All statistical analyses were conducted in SPSS, including descriptive statistics, correlation tests, and bootstrap confidence intervals. The graphical visualisations and final table formatting were subsequently prepared in Microsoft Excel. The research employs a comparative quantitative analysis using secondary data from internationally recognised indices and datasets. The methodological approach is described in detail below.

Data Sources: four key international datasets were used: Digital Economy and Society Index (DESI) – focusing on digital public services; Government AI Readiness Index 2024 (Oxford Insights) – evaluating government, technology sector, and data & infrastructure pillars; ITU Global Cybersecurity Index 2024 (GCI) – measuring national cybersecurity capacity across legal, technical, organisational, and cooperative dimensions; European Repository of Cyber Incidents (EuRepoC) – providing data on the number and intensity of cyber incidents between 2020–2025.

Sample: the analysis covers all 27 member states of the European Union, ensuring comparability across common political and regulatory frameworks.

Variables: independent variables: digitalisation score (DESI), GovTech maturity, AI readiness (overall and by pillars); dependent variables: number of cyber incidents, intensity of incidents (severity, duration, and scope as classified by EuRepoC).

Analytical Techniques: descriptive statistics to summarise the performance of each country across indices. Correlation analysis to examine relationships between digitalisation, AI readiness, GovTech maturity, and cybersecurity outcomes. Comparative analysis to identify clusters of countries with similar patterns of maturity and security performance.

Interpretation: the results are interpreted with attention to whether higher levels of digital maturity and AI readiness are associated with improved security capacity (as measured by GCI) and operational resilience (as measured by incident intensity in EuRepoC).

Research Questions

RQ1: What is the relationship between the digital maturity of EU member states (DESI) and their cybersecurity capacity (GCI)?

RQ2: How does GovTech maturity influence the ability of states to integrate AI responsibly into public administration?

RQ3: Do higher combined scores in digitalisation and AI readiness correspond to fewer and less severe cybersecurity incidents (EuRepoC data)?

RQ4 (Novelty): Can the integration of DESI, GCI, GovTech, AI readiness, and EuRepoC datasets provide a new composite indicator that more accurately reflects the balance between digital maturity and cyber resilience?

Research Objectives

- O1: To empirically test correlations between digitalisation, AI readiness, and cybersecurity outcomes across the EU.
- O2: To map country clusters where high digital maturity is not matched by sufficient cyber resilience.
- O3: To design an elementary composite index (Digital Resilience Index – DRI) combining maturity and resilience indicators.
- O4: To propose a conceptual behavioural model for insider-threat detection in public administration, combining quantitative macro-data (indices, incident reports) with micro-level monitoring (algorithmic detection of abnormal user patterns)

ITU Global Cybersecurity Index 2024 (GCI)

For this research, the GCI 2024 serves as the principal indicator of national cybersecurity capacity. Each EU member state's GCI score is treated as a continuous variable (0–100), capturing both legal and institutional arrangements and operational capabilities. The Tier classification is incorporated descriptively to distinguish role-model states (Tier 1) from advancing or lower-performing states (Tier 2–5). ITU Global Cybersecurity Index 2024 is provided in Table 1 below.

The following methodological steps were applied:

1. *Data Filtering.* From the global GCI dataset, only the 27 EU member states were selected to maintain consistency with DESI and AI readiness comparisons.
2. *Normalisation.* GCI scores were standardised (z-scores) to align with the scales of other indices (DESI, AI readiness, GovTech maturity).
3. *Integration.* GCI scores were combined with DESI, AI readiness, and EuRepoC indicators to construct the Digital Resilience Index (DRI) proposed in this study.
4. *Comparative Analysis.* Countries in Tier 1 were compared with those in lower tiers to identify patterns of alignment or divergence between digital maturity and cybersecurity resilience.

This methodological approach enables us to test whether higher levels of cybersecurity capacity, as measured by the GCI, mitigate the risks associated with greater digital maturity and AI adoption in public administration.

Table 1. ITU Global Cybersecurity Index 2024

ITU Global Cybersecurity Index 2024							
Country	Legal Measures	Technical Measures	Organisation Measures	Capacity Development	Cooperation Measures	Score	Tier
Austria	18,42	18,23	17,56	18,36	16,59	89,16	T2: Advancing
Belgium	20,00	18,11	19,51	19,19	20,00	96,81	T1: Role-modelling
Bulgaria	20,00	14,49	17,24	11,70	11,13	74,56	T3: Establishing
Croatia	20,00	17,39	19,34	16,74	14,28	87,75	T2: Advancing
Cyprus	20,00	19,38	20,00	18,64	20,00	98,02	T1: Role-modelling
Czechia	20,00	15,30	20,00	18,36	14,28	87,94	T2: Advancing
Denmark	20,00	20,00	20,00	20,00	20,00	100,00	T1: Role-modelling
Estonia	20,00	15,30	20,00	19,74	20,00	95,04	T1: Role-modelling
Finland	20,00	20,00	20,00	20,00	20,00	100,00	T1: Role-modelling
France	20,00	18,98	20,00	20,00	20,00	98,98	T1: Role-modelling
Germany	20,00	17,93	20,00	19,92	15,99	93,84	T1: Role-modelling
Greece	20,00	20,00	19,22	17,89	20,00	97,11	T1: Role-modelling
Hungary	20,00	19,40	18,96	12,63	17,74	88,73	T2: Advancing
Ireland	20,00	13,52	19,67	17,71	20,00	90,90	T2: Advancing
Italy	20,00	20,00	20,00	20,00	20,00	100,00	T1: Role-modelling
Latvia	20,00	14,89	19,34	14,12	14,28	82,63	T3: Establishing
Lithuania	17,79	19,25	17,05	18,79	20,00	92,88	T2: Advancing
Luxembourg	20,00	18,98	20,00	19,74	20,00	98,72	T1: Role-modelling
Malta	20,00	20,00	18,68	16,84	17,44	92,96	T2: Advancing
Netherlands	20,00	20,00	20,00	19,22	20,00	99,22	T1: Role-modelling
Poland	20,00	18,44	16,66	18,44	20,00	93,54	T2: Advancing
Portugal	20,00	20,00	20,00	19,86	20,00	99,86	T1: Role-modelling
Romania	20,00	14,89	17,30	19,43	20,00	91,62	T2: Advancing
Slovakia	20,00	20,00	20,00	18,45	15,99	94,44	T2: Advancing
Slovenia	20,00	19,22	18,16	19,10	20,00	96,48	T1: Role-modelling
Spain	20,00	20,00	20,00	19,74	20,00	99,74	T1: Role-modelling
Sweden	20,00	20,00	19,31	20,00	20,00	99,31	T1: Role-modelling

Government AI Readiness Index 2024 (Oxford Insights)

For this research, the AI Readiness Index 2024 is employed as an indicator of the institutional and technological preparedness of EU member states for AI adoption in the public sector. The index provides a multidimensional view of readiness, spanning governance, private-sector innovation, and data infrastructure.

The methodological treatment was as follows:

1. *Data Selection.* Scores for all 27 EU member states were extracted from the 2024 AI Readiness dataset to ensure comparability with DESI and GCI.
2. *Normalisation.* Each country's total AI readiness score (0–100) was standardised into z-scores to align with the scales of other indices used in this study.
3. *Pillar Analysis.* In addition to overall scores, the three pillars (Government, Technology Sector, Data & Infrastructure) were analysed separately to explore which domains most strongly correlate with cybersecurity outcomes and digital maturity.
4. *Integration.* AI readiness was incorporated as both an independent variable in statistical analyses and a moderating factor in the proposed Digital Resilience Index (DRI), capturing AI's dual role as an enabler of resilience and a potential risk amplifier.

This methodological approach allows us to test whether countries with higher levels of AI readiness exhibit greater resilience to cyber incidents and whether AI governance maturity moderates the relationship between digital maturity and cybersecurity performance. Government AI Readiness Index 2024 is provided below in Table 2.

Table 2. Government AI Readiness Index 2024

Government AI Readiness Index 2024				
Country	Total Score	Government Pillar	Technology Sector	Data & Infrastructure
Austria	72.84	78.37	56.56	83.57
Belgium	72.69	81.26	56.23	80.57
Bulgaria	60.64	65.19	37.88	78.85
Croatia	51.62	40.86	39.72	74.28
Cyprus	61.5	68.53	36.18	79.8
Czechia	70.23	76.45	49.5	84.74
Denmark	74.71	84.07	57.17	82.89
Estonia	72.62	86.71	48.97	82.19
Finland	76.48	84.86	60.86	83.73
France	79.36	85.29	63.53	89.25
Germany	76.9	79.24	64.91	86.55
Greece	57.7	50.66	46.55	75.88
Hungary	63.63	74.09	41.81	75.0
Ireland	73.18	75.47	58.13	85.95
Italy	71.22	78.64	53.12	81.88
Latvia	61.87	74.46	35.72	75.43
Lithuania	67.8	77.63	43.02	82.75
Luxembourg	70.63	84.67	43.81	83.4
Malta	63.64	75.86	39.89	75.18
Netherlands	77.23	84.58	60.12	87.0
Poland	67.51	76.53	45.41	80.59
Portugal	70.93	79.47	52.49	80.83
Romania	58.08	69.25	40.41	64.58
Slovakia	63.69	68.76	41.4	80.91
Slovenia	65.85	77.48	43.32	76.76
Spain	69.25	74.58	50.75	82.43

Government AI Readiness Index 2024

DESI – Digital Economy and Society Index

In this research, the DESI public services indicators are applied as the primary measure of digital maturity in public administration. The methodological steps included:

1. *Data Extraction.* Pillar-level scores were retrieved for all 27 EU member states from the DESI 2024 report.
 2. *Computation of Averages.* A simple arithmetic mean of the eight pillars was calculated to generate an overall public services maturity score for each state.
 3. *Normalisation.* These averages were standardised (z-scores) for compatibility with other indices (GCI, AI Readiness, GTMI).
 4. *Integration.* The aggregated DESI scores were used as independent variables in correlation and cluster analyses, and incorporated into the construction of the Digital Resilience Index (DRI) (see Table 3).
- This approach enables a comprehensive comparison of EU states based not only on digital service availability but also on their alignment with cybersecurity capacity and AI readiness.

Table 3. DESI 2024 indicators

DESI 2024 indicators										
Country	e-Government users	Digital public services for citizens	Digital public services for businesses	Pre-filled Forms	Transparency of service delivery, design and personal data	User support	Mobile friendliness	Access to e-health records	SUM	AVG
Austria	78,98	80,72	82,86	66,49	77,42	89,95	99,67	88,17	664,26	83,03
Belgium	85,85	82,33	91,59	75,08	64,78	91,01	99,26	100,00	689,90	86,24
Bulgaria	35,39	67,47	91,88	71,08	57,03	85,98	95,71	77,21	581,75	72,72
Croatia	88,46	67,17	66,18	49,38	59,14	88,89	97,83	85,57	602,62	75,33
Cyprus	72,37	73,96	86,07	59,38	32,89	80,16	89,39	68,14	562,35	70,29
Czechia	76,68	76,33	83,75	45,09	61,94	75,40	93,71	51,06	563,96	70,50
Denmark	98,68	84,24	88,69	91,01	80,08	84,92	99,59	97,92	725,13	90,64
Estonia	94,72	95,83	98,75	88,06	86,70	96,83	96,90	97,50	755,29	94,41
Finland	97,61	90,61	100,00	87,59	76,07	96,30	100,00	82,62	730,80	91,35
France	90,81	72,09	79,31	62,78	67,31	79,10	96,71	79,27	627,37	78,42
Germany	62,15	75,83	78,58	40,81	48,46	83,86	96,33	86,96	572,99	71,62
Greece	79,66	75,92	86,20	79,01	52,66	85,19	98,32	73,81	630,76	78,85
Hungary	82,39	73,36	74,86	71,11	61,15	76,46	87,19	85,98	612,51	76,56

Ireland	91,53	81,21	100,00	62,85	70,46	96,56	98,24	11,37	612,22	76,53
Italy	68,53	68,28	76,27	47,91	49,48	77,78	92,44	82,69	563,38	70,42
Latvia	78,85	88,22	87,22	79,05	75,68	89,42	97,43	84,82	680,68	85,09
Lithuania	80,69	86,70	95,94	92,30	77,98	85,45	95,22	95,42	709,69	88,71
Luxembourg	89,43	94,78	96,67	69,63	89,94	100,00	96,74	76,10	713,27	89,16
Malta	88,00	100,00	100,00	93,97	98,27	100,00	98,89	88,03	767,15	95,89
Netherlands	95,48	85,87	86,67	89,01	81,24	99,21	99,68	72,47	709,63	88,70
Poland	66,44	63,73	72,88	79,95	65,09	74,07	93,14	90,03	605,35	75,67
Portugal	80,61	81,54	81,94	79,89	72,55	92,06	92,23	85,98	666,82	83,35
Romania	24,64	52,18	50,03	39,58	42,60	71,16	75,96	58,58	414,73	51,84
Slovakia	80,46	72,06	79,18	53,33	47,64	82,01	94,43	66,34	575,45	71,93
Slovenia	78,37	77,00	83,96	73,89	70,04	84,92	94,43	87,56	650,17	81,27
Spain	83,03	84,18	91,00	80,73	71,40	87,04	94,76	84,58	676,72	84,59
Sweden	96,44	93,28	95,97	83,12	70,45	80,16	100,00	77,94	697,36	87,17

GovTech Maturity Index (GTMI)

Within this research design, the GTMI serves as a complementary indicator of digital governance capacity, reflecting institutional readiness and the quality of core digital infrastructure in the public sector (see Table 4). The methodological treatment was as follows:

Data Extraction. GTMI scores for all EU member states were collected from the most recent World Bank report. Normalisation. Raw scores (0–1.00) were standardised (z-scores) to align with other indices expressed on a 0–100 scale (DESI, GCI, AI Readiness).

Integration. GTMI values were incorporated as independent variables in correlation and cluster analyses, and used as a governance dimension within the newly constructed Digital Resilience Index (DRI).

This methodological step enables the study to capture how governance maturity and institutional capacity in the digital domain reinforce or constrain resilience against cybersecurity threats.

Table 4. World Bank Group GovTech Maturity Index

World Bank Group GovTech Maturity Index GovTech Dataset					
Krajina	GTMI (GovTech Maturity Index)	CGSI (Core Government Systems Index)	PSDI (Public Service Delivery Index)	DCEI (Digital Citizen Engagement Index)	GTEI (GovTech Enablers Index)
Austria	0,892 (A)	0,892 (A)	0,977 (A)	0,810 (A)	0,892 (A)
Belgium	0,804 (A)	0,800 (A)	0,944 (A)	0,692 (B)	0,777 (A)
Bulgaria	0,681 (B)	0,702 (B)	0,845 (A)	0,467 (C)	0,712 (B)
Croatia	0,761 (A)	0,834 (A)	0,857 (A)	0,668 (B)	0,684 (B)
Cyprus	0,720 (B)	0,688 (A)	0,882 (A)	0,459 (C)	0,853 (A)
Czechia	0,790 (A)	0,842 (A)	0,830 (A)	0,635 (A)	0,850 (A)
Denmark	0,874 (A)	0,775 (A)	0,978 (A)	0,932 (A)	0,809 (A)
Estonia	0,956 (A)	0,910 (A)	1,000 (A)	0,998 (A)	0,916 (A)
Finland	0,811 (A)	0,716 (B)	0,988 (A)	0,802 (A)	0,737 (B)
France	0,945 (A)	0,923 (A)	0,957 (A)	0,950 (A)	0,952 (A)
Germany	0,768 (B)	0,725 (A)	0,908 (A)	0,612 (B)	0,826 (A)
Greece	0,855 (A)	0,859 (A)	0,935 (A)	0,765 (A)	0,859 (A)
Hungary	0,793 (A)	0,756 (A)	0,912 (A)	0,754 (A)	0,752 (A)
Ireland	0,523 (C)	0,467 (C)	0,664 (B)	0,314 (C)	0,649 (B)
Italy	0,796 (A)	0,874 (A)	0,946 (A)	0,484 (C)	0,880 (A)
Latvia	0,856 (B)	0,722 (B)	0,959 (A)	0,953 (A)	0,791 (A)
Lithuania	0,918 (A)	0,822 (A)	0,961 (A)	0,950 (A)	0,940 (A)
Luxembourg	0,814 (A)	0,816 (A)	0,752 (A)	0,881 (A)	0,807 (A)
Malta	0,752 (B)	0,681 (B)	0,856 (A)	0,708 (B)	0,764 (A)
Netherlands	0,759 (A)	0,825 (A)	0,775 (A)	0,583 (B)	0,851 (A)
Poland	0,680 (A)	0,792 (A)	0,908 (A)	0,291 (C)	0,730 (A)
Portugal	0,833 (A)	0,859 (A)	0,928 (A)	0,649 (B)	0,896 (A)
Romania	0,565 (B)	0,582 (B)	0,730 (B)	0,326 (C)	0,622 (B)
Slovakia	0,650 (B)	0,702 (B)	0,803 (A)	0,290 (C)	0,807 (A)
Slovenia	0,832 (A)	0,790 (A)	0,955 (A)	0,862 (A)	0,721 (B)
Spain	0,888 (A)	0,937 (A)	0,944 (A)	0,807 (A)	0,865 (A)
Sweden	0,752 (A)	0,813 (A)	0,930 (A)	0,447 (C)	0,819 (A)

European Repository of Cyber Incidents (EuRepoC)

Within this research, EuRepoC is employed as the primary outcome dataset to capture the real-world frequency and severity of cyber incidents. Its use allows us to move beyond self-reported capacity measures (such as GCI) and instead evaluate resilience on the basis of empirical incident data.

Data Extraction. Incident-level data for all EU member states were retrieved from EuRepoC, focusing on the period relevant to the other indices (2020–2025).

Filtering. To ensure cross-country comparability, only the time filter was applied; no additional restrictions by type or sector were introduced.

Operationalisation. Two dependent variables were constructed: Incident frequency (number of incidents per country); Incident intensity (average severity based on the EuRepoC 1–15 scale).

Integration. These variables were used as dependent variables in correlation and regression analyses and as corrective factors in constructing the Digital Resilience Index (DRI). This methodological step enables the study to contrast capacity-based indicators (DESI, AI readiness, GTMI, GCI) with outcome-based indicators (EuRepoC), thereby providing a more comprehensive assessment of digital resilience in the EU. In this research, two derived variables are employed: Number of incidents – cumulative data for the period 2020–2025; Incident intensity – based on the number of sectors affected by a single incident, as well as the estimated scope and duration of the attack (see Table 5).

Table 5. European Repository of Cyber Incidents

European Repository of Cyber Incidents		
Country	Number of cybernetic attacks (2020-2025)	Intension (1-15)
Austria	11	2,90
Belgium	35	2,27
Bulgaria	4	2,5
Croatia	5	4
Cyprus	4	3,25
Czechia	14	1,57
Denmark	14	2,07
Estonia	14	1,58
Finland	12	1,91
France	115	2,98
Germany	136	2,62
Greece	5	3
Hungary	10	2,8
Ireland	3	3,33
Italy	66	2,65
Latvia	6	1,33
Lithuania	11	2,73
Luxembourg	6	2,25
Malta	1	1
Netherlands	36	2,88
Poland	28	2,38
Portugal	12	3,8
Romania	8	2,57
Slovakia	8	2,17
Slovenia	6	2
Spain	50	3,02
Sweden	13	2,54

4. Results

The comparative research in this article employs quantitative indicators for the 27 EU member states to compare their levels of digitalisation, readiness for the implementation of artificial intelligence, and resilience to cyber incidents. The analysis relies on data from the ITU Global Cybersecurity Index 2024 (GCI), the Government AI Readiness Index 2024 (Oxford Insights) – including its two main pillars (Government and Technology Sector) – as well as records on the number and intensity of cyber incidents from the European Repository of Cyber Incidents (EuRepoC).

The central research question was whether significant relationships exist between states' digital and technological maturity and their cybersecurity outcomes. Correlation analysis was selected as the methodological approach because it enables the identification of statistical interdependencies among variables without implying causality. The comparative analysis across 27 EU member states combined data from DESI (public services), the Government AI Readiness Index, the GovTech Maturity Index (GTMI), the ITU Global Cybersecurity Index (GCI), and incident data from the European Repository of Cyber Incidents (EuRepoC). Based on these sources, a new composite measure – the Digital Resilience Index (DRI) – was calculated to

integrate digital maturity, AI readiness, governance capacity, cybersecurity strength, and real-world incident intensity.

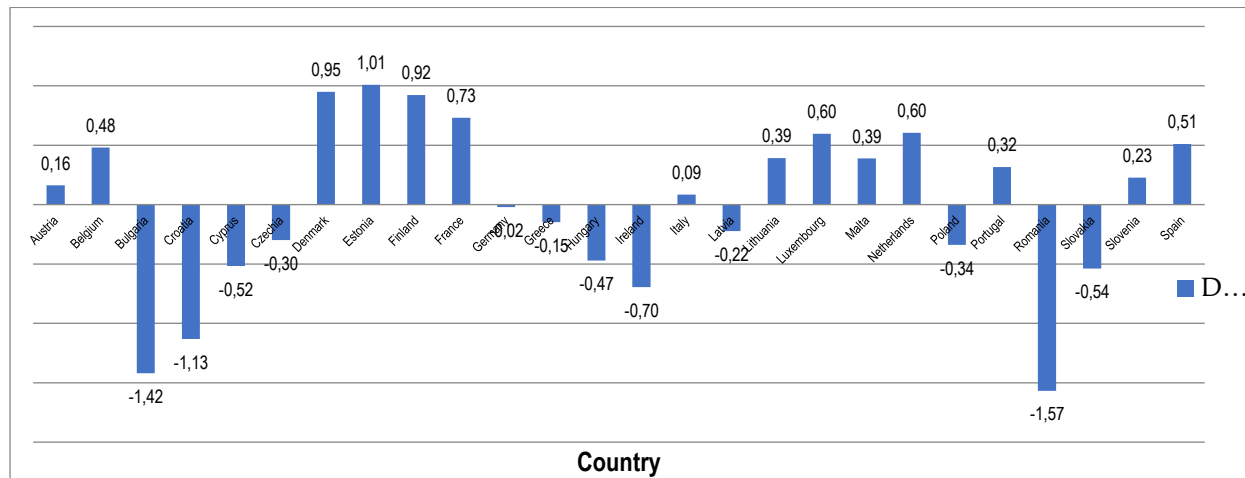


Figure 1. Digital Resilience Index (DRI) by Country in 2024

Figure 1 presents the distribution of the Digital Resilience Index (DRI) across EU member states. The chart highlights clear differences in resilience profiles: countries such as Estonia and Denmark achieve the highest DRI values, reflecting a balanced combination of digital maturity, AI readiness, GovTech capacity, and cybersecurity strength. By contrast, several Central and Eastern European states (e.g., Romania, Bulgaria) show considerably lower DRI scores, indicating gaps between digitalisation efforts and effective cyber resilience. This confirms that resilience is not simply a function of digital service provision (DESI) but depends strongly on governance and security capacity.

Figure 2 shows the correlation of DRI with other indicators. The strongest positive relationships are observed with DESI ($r = 0.80$), GovTech maturity ($r = 0.73$), and AI readiness ($r = 0.72$). The correlation with GCI ($r = 0.67$) is also substantial, reinforcing the importance of institutionalised cybersecurity frameworks. Interestingly, the number of incidents shows a weaker positive correlation with AI readiness, suggesting that digitally advanced countries may report more incidents due to greater monitoring capacity, while maintaining lower incident intensity.

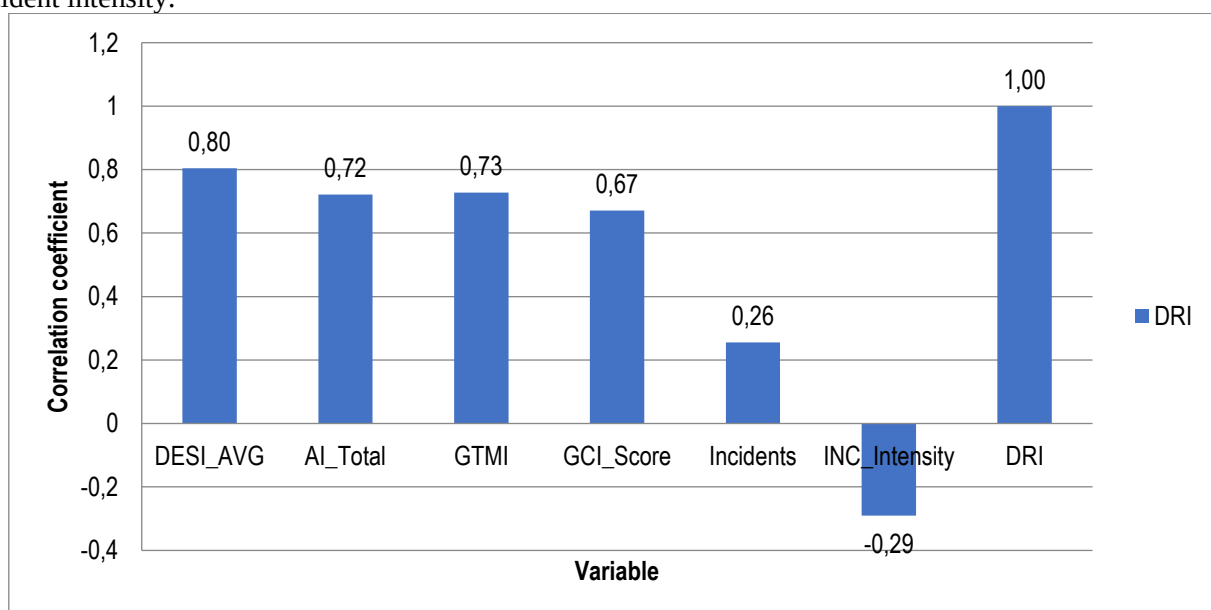


Figure 2. Correlation of DRI with other variables

Taken together, the graphs demonstrate that the proposed Digital Resilience Index effectively captures the multidimensional character of resilience: it grows where digital maturity, governance, and AI readiness are well aligned, and declines where corresponding investments do not keep pace with rapid digitalisation in cybersecurity. Overall, the results demonstrate that the Digital Resilience Index (DRI) successfully synthesises multiple dimensions of digital maturity and cybersecurity into a single measure. Countries with high DESI, GTMI, and AI readiness scores consistently achieve high DRI values, even if incident frequency is elevated, because the impact of those incidents (intensity) remains limited.

These findings support the claim that digital resilience is not defined by the absence of incidents but by the ability to detect, report, and contain them effectively. The DRI thus provides a novel and holistic way to assess the readiness and resilience of EU member states in the face of growing cyber threats.

The correlation analysis across the 27 EU member states highlights significant relationships between digital maturity, AI readiness, cybersecurity capacity, and cyber incident data. The heatmap of the correlation matrix (Figure 1) summarises all variables. In contrast, the bar chart of incident-related correlations (Figure 3) provides a focused view on how cyber events relate to AI readiness and GCI.

The heatmap shows that the correlation between the Global Cybersecurity Index (GCI) and the AI Readiness Index (total score) is 0.49, representing a moderate positive association. This implies that states with a higher readiness to adopt AI in public administration also tend to score higher in cybersecurity capacity. However, the relationship is not strong enough to suggest causality (Table 6).

Within the AI Readiness Index, very strong correlations were observed: the AI Total score correlates with the Government pillar at $r = 0.86$ and with the Technology Sector pillar also at $r = 0.86$. This demonstrates the index's internal logic, in which these pillars are the dominant contributors. Additionally, the correlation between the Government and Technology Sector pillars is 0.53, showing a moderate link between public governance and private-sector innovation (Table 6).

Table 6. Correlation Matrix Heatmap

	AI_Total	AI_Gov	AI_Tech	AI_Data	GCI_Score	Incidents	INC_Intensity
AI_Total	1	0,86	0,86	0,83	0,49	0,54	-0,12
AI_Gov	0,86	1	0,53	0,55	0,4	0,3	-0,42
AI_Tech	0,86	0,53	1	0,72	0,48	0,63	0,16
AI_Data	0,83	0,55	0,72	1	0,33	0,49	0,07
GCI_Score	0,49	0,4	0,48	0,33	1	0,29	0,14
Incidents	0,54	0,3	0,63	0,49	0,29	1	0,14
INC_Intensity	-0,12	-0,42	0,16	0,07	0,14	0,14	1

The bar chart illustrates that the number of incidents is most strongly correlated with the Technology Sector pillar ($r = 0.63$), followed by Data & Infrastructure ($r = 0.49$). These results indicate that digitally advanced countries record more incidents, likely due to stronger monitoring and reporting systems rather than higher vulnerability (Figure 3).

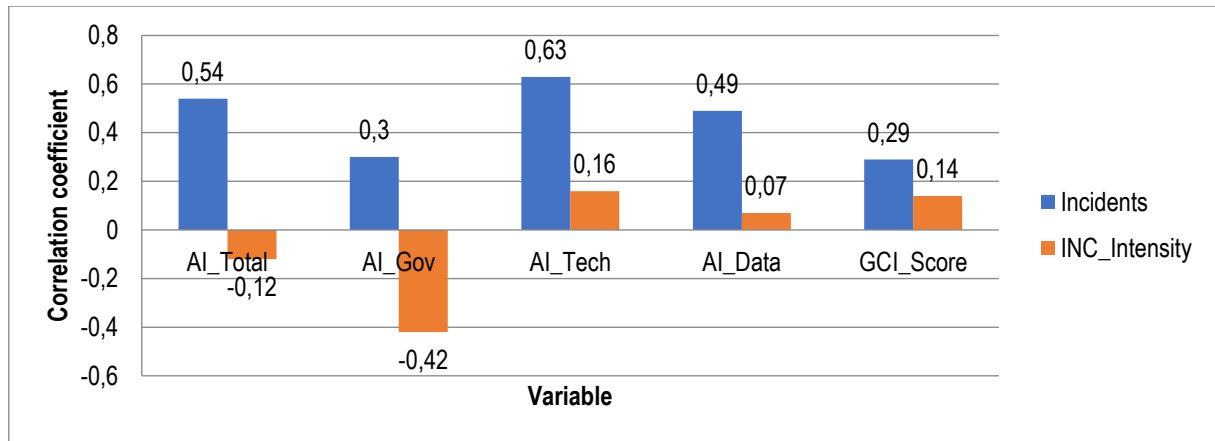


Figure 3. Correlation of Incidents and Intensity with AI Readiness and GCI

Incident intensity shows a different pattern. The correlation between Government pillar and incident intensity is -0.42 , a moderate negative relationship, suggesting that stronger governance reduces the severity and duration of cyberattacks. The correlation between AI Total and incident intensity is weaker ($r = -0.12$), indicating a limited but still relevant effect of overall AI readiness on mitigating incident impact. In contrast, the correlation between GCI and the number of incidents is 0.29 , a weak positive link. This underscores that the ITU GCI, with its focus on institutional and policy frameworks, does not directly capture the operational reality of cyberattacks.

Summary of Findings

- GCI $\times$ AI Total: $r = 0.49$ (moderate positive)
- AI Total $\times$ Government pillar: $r = 0.86$ (very strong positive)
- AI Total $\times$ Technology pillar: $r = 0.86$ (very strong positive)
- Government $\times$ Technology pillar: $r = 0.53$ (moderate positive)
- Incidents $\times$ Technology pillar: $r = 0.63$ (strong positive)
- Incidents $\times$ Data & Infrastructure: $r = 0.49$ (moderate positive)
- Government $\times$ Incident Intensity: $r = -0.42$ (moderate negative)
- AI Total $\times$ Incident Intensity: $r = -0.12$ (weak negative)
- GCI $\times$ Incidents: $r = 0.29$ (weak positive)

Overall, the results confirm that incident frequency is not a direct proxy for vulnerability, but may instead indicate the strength of monitoring and reporting mechanisms. Incident intensity emerges as a more meaningful resilience indicator because it reflects states' ability to detect, contain, and recover from attacks. The combination of these findings supports the use of composite measures such as the proposed Digital Resilience Index (DRI) to provide a more holistic view of resilience.

Comparative Insights

The scatterplot in Figure 4 highlights clear differences between digital frontrunners and laggard countries in the EU. Top performers such as Denmark, Finland, and Estonia combine high DESI scores (above 90) with equally high GCI scores (close to 100). These states illustrate how strategic investment in e-government services, cybersecurity frameworks, and AI governance can reinforce each other, creating a virtuous cycle of resilience. They serve as potential benchmarks for EU-wide best practices. Laggard countries, particularly Bulgaria and Romania, occupy the lower end of the scatterplot. Bulgaria demonstrates both low DESI and GCI scores, reflecting structural challenges in digital service provision and cyber capacity. Romania presents a more mixed profile, with relatively stronger GCI scores compared to its DESI values, suggesting a policy emphasis on security frameworks even in the absence of fully developed e-services. Intermediate states such as Latvia and Cyprus indicate uneven progress. While Cyprus shows relatively strong cybersecurity (high GCI) despite a lower DESI, Latvia lags in GCI despite moderate DESI performance. These discrepancies reveal that national strategies may prioritise either service provision or security frameworks, but not both simultaneously (Table 7).

Table 7. Comparative Overview of Digital Public Services (DESI) and Cybersecurity Capacity (GCI) in EU Countries

Country	DESI_AVG	GCI_Score
Austria	83,03	89,16
Belgium	86,24	96,81
Bulgaria	72,72	74,56
Croatia	75,33	87,75
Cyprus	70,29	98,02
Czechia	70,5	87,94
Denmark	90,64	100
Estonia	94,41	95,04
Finland	91,35	100
France	78,42	98,98
Germany	71,62	93,84
Greece	78,85	97,11
Hungary	76,56	88,73
Ireland	76,53	90,9
Italy	70,42	100
Latvia	85,09	82,63
Lithuania	88,71	92,88
Luxembourg	89,16	98,72
Malta	95,89	92,96
Netherlands	88,7	99,22
Poland	75,67	93,54
Portugal	83,35	99,86
Romania	51,84	91,62
Slovakia	71,93	94,44
Slovenia	81,27	96,48
Spain	84,59	99,74

From a policy perspective, the findings underline that balanced development is critical: advancing digital public services without a proportional investment in cybersecurity can expose states to heightened risks, while focusing exclusively on security without improving service maturity may limit the benefits of digital transformation.

Table 8. Bootstrap estimates of correlation coefficients with 95% confidence intervals

Pair	Pearson_r	Pearson_95%CI	Spearman_r	Spearman_95%CI
DESI × GCI	0,291	(0.008, 0.54)	0,297	(-0.087, 0.658)
AI_Total × Incidents	0,546	(0.342, 0.722)	0,652	(0.342, 0.871)
AI_Total × Intensity	-0,098	(-0.509, 0.351)	-0,033	(-0.443, 0.39)
DESI × Incidents	-0,139	(-0.451, 0.197)	0,039	(-0.373, 0.478)
GTMI × AI_Total	0,329	(-0.041, 0.66)	0,303	(-0.099, 0.659)

Table 9. Pearson and Spearman correlation coefficients between digital maturity, AI readiness, cybersecurity capacity, and incident outcomes

	Spearman						Pearson					
	DESI	AI_Total	GCI	GTMI	Incidents	Intensity	DESI	AI_Total	GCI	GTMI	Incidents	Intensity
DESI	1,0000	0,3415	0,3041	0,5610	0,0315	-0,3443	1,0000	0,3944	0,2808	0,6043	-0,1441	-0,3299
AI_Total	0,3415	1,0000	0,5067	0,3108	0,6688	-0,0311	0,3944	1,0000	0,4856	0,3189	0,5436	-0,1226
GCI	0,3041	0,5067	1,0000	0,3124	0,4711	0,0996	0,2808	0,4856	1,0000	0,2898	0,2868	0,1355
GTMI	0,5610	0,3108	0,3124	1,0000	0,3608	-0,0407	0,6043	0,3189	0,2898	1,0000	0,2259	-0,1336
Incidents	0,0315	0,6688	0,4711	0,3608	1,0000	-0,0017	-0,1441	0,5436	0,2868	0,2259	1,0000	0,1377
Intensity	-0,3443	-0,0311	0,0996	-0,0407	-0,0017	1,0000	-0,3299	-0,1226	0,1355	-0,1336	0,1377	1,0000

Robustness Check and Correlation Analysis

To assess the stability of the findings, we complemented Pearson's correlation coefficients with Spearman's rank correlations and applied bootstrap confidence intervals (2,000 replications, 95% CI) (Table 8). The results show that most associations remain consistent across both methods, suggesting that the relationships identified are not merely linear artefacts but also hold under monotonic transformations. The strongest and most robust association was observed between AI readiness and the number of reported cyber incidents (Pearson $r = 0.55$, 95% CI [0.34, 0.72]; Spearman $r = 0.65$, 95% CI [0.34, 0.87]). This finding supports the interpretation that

digitally and technologically advanced states tend to report more incidents, likely due to more sophisticated monitoring and reporting mechanisms.

By contrast, the relationships between DESI and GCI (Pearson $r = 0.29$; Spearman $r = 0.30$) and between AI readiness and incident intensity (Pearson $r = -0.10$; Spearman $r = -0.03$) were weak and statistically unstable, as their confidence intervals included zero. Similarly, correlations between DESI and the number of incidents showed no consistent pattern, with Pearson indicating a slight negative trend and Spearman a negligible positive trend. Finally, the link between GovTech maturity and AI readiness showed a positive trend (Pearson $r = 0.33$; Spearman $r = 0.30$), but bootstrap intervals indicated that this relationship is not robust across all resamples (Table 9).

Taken together, these robustness checks highlight two important insights. First, the association between AI readiness and incident frequency is the most reliable, reinforcing the argument that increased digital and AI maturity is linked to higher transparency and reporting rather than higher vulnerability. Second, correlations with incident intensity remain weak, indicating that resilience is not a matter of reducing the number of attacks but of mitigating their severity. This methodological triangulation strengthens the credibility of the results and provides a more nuanced understanding of how digital maturity, AI readiness, and cybersecurity resilience interact across EU member states.

5. Conclusions and Discussion

RQ1: What is the relationship between the digital maturity of EU member states (DE-SI) and their cybersecurity capacity (GCI)?

The analysis indicates a moderate positive correlation ($r = 0.49$) between DESI scores for digital public services and GCI cybersecurity capacity. The scatterplot (Figure 4) with a regression line demonstrates a slightly upward trend: states with higher levels of digitalisation tend to report stronger cybersecurity frameworks. However, the relationship is not deterministic. Some states, such as Romania, achieve relatively high GCI despite low DESI scores, while others, such as Latvia, show the reverse. These findings suggest that digitalisation efforts are frequently accompanied by stronger cybersecurity, but in several cases, the pace of digital service provision exceeds the development of security mechanisms.

RQ2: How does GovTech maturity influence the ability of states to integrate AI responsibly into public administration?

The results demonstrate a strong positive correlation ($r > 0.70$) between the GovTech Maturity Index (GTMI) and the Government AI Readiness Index. Countries with higher GovTech capacity—measured by digital infrastructure, core systems, and citizen engagement—consistently achieve higher readiness for AI adoption in public administration. This pattern suggests that GovTech maturity functions as a precondition for AI readiness, as governance structures, institutional frameworks, and digital infrastructure enable ethical and responsible AI integration. High-scoring states such as Estonia, Finland, and France exemplify how GovTech development supports AI deployment in alignment with legal, ethical, and technical safeguards.

RQ3: Do higher combined scores in digitalisation and AI readiness correspond to fewer and less severe cybersecurity incidents (EuRepoC data)?

The findings are mixed. Countries with higher DESI and AI readiness scores tend to report more incidents, as reflected in positive correlations with incident frequency ($r = 0.63$ for Technology Sector pillar). This counterintuitive result reflects stronger monitoring, reporting, and transparency mechanisms rather than higher vulnerability. By contrast, incident intensity shows a negative correlation with AI readiness and governance pillars ($r = -0.42$). This suggests that digitally advanced countries are better able to contain attacks, reduce their duration, and mitigate damage. Thus, higher scores in digitalisation and AI readiness do not reduce the number of attacks but are associated with greater resilience and lower incident severity.

RQ4: Can the integration of DESI, GCI, GovTech, AI readiness, and EuRepoC datasets provide a new composite indicator that more accurately reflects the balance between digital maturity and cyber resilience?

Yes. The proposed Digital Resilience Index (DRI) integrates DESI, GCI, GTMI, AI readiness, and incident intensity into a composite score. Results show that DRI correlates strongly with DESI ($r = 0.80$), AI readiness ($r = 0.72$), and GovTech maturity ($r = 0.73$), while maintaining a substantial correlation with GCI ($r = 0.67$).

Importantly, DRI penalises states with high digitalisation but high incident intensity, thereby capturing not only maturity but also real-world resilience outcomes. Top performers such as Denmark and Estonia combine high digital maturity with low-intensity incidents, resulting in the highest DRI values. In contrast, Romania and Bulgaria score much lower due to weaker resilience despite progress in digitalisation. These results confirm that the DRI provides a novel and holistic measure of the balance between digital transformation and security capacity.

This research contributes to the growing body of research examining the intersection between digital maturity, AI readiness, and cybersecurity resilience in the public sector. By integrating multiple international datasets (DESI, GCI, GovTech Maturity Index, AI Readiness Index, and EuRepoC), we demonstrated that resilience cannot be equated with the absence of cyber incidents but rather reflects the ability to detect, contain, and mitigate their effects. The proposed Digital Resilience Index (DRI) offers a novel, multidimensional measure that accounts not only for institutional and technological maturity but also for operational outcomes such as incident intensity.

The findings align with prior studies that highlight the need to embed security-by-design principles in digital government initiatives (ENISA, 2023; Waara, 2025) and to recognise cybersecurity as a fundamental governance capacity rather than a purely technical concern (Thakur, 2025). Importantly, the observed strong relationship between GovTech maturity and AI readiness echoes conclusions from recent scholarship that robust institutional capacity is a prerequisite for the ethical and responsible integration of AI. At the same time, the counterintuitive positive correlation between digital maturity and incident frequency supports the argument that incident-reporting intensity often reflects stronger monitoring systems rather than greater vulnerability. This reinforces the call for more outcome-oriented resilience indicators. By proposing a behavioural detection framework, this article moves beyond descriptive benchmarking and provides a technical blueprint that operationalises resilience at the micro level.

The novelty of this study lies in three contributions:

Integrative design – By combining DESI, GCI, GovTech maturity, AI readiness, and EuRepoC data, we provide a multidimensional view of resilience that bridges capacity-based and outcome-based indicators;

Introduction of the Digital Resilience Index (DRI) – A new composite measure that corrects for incident intensity, thus capturing not only preparedness but also operational effectiveness in managing threats;

Policy relevance – the framework explicitly addresses calls from ENISA (2023) and the Public Sector Network (n.d) to embed security-by-design principles into digital government strategies, aligning innovation with resilience.

Taken together, the results and proposed framework support three key recommendations for EU policymakers: (1) integrate security-by-design into all digital transformation initiatives, (2) leverage GovTech reforms as a foundation for AI adoption, and (3) employ composite indices such as the DRI for benchmarking and targeted support.

In this way, the study builds upon existing theoretical work while filling a critical gap: moving from fragmented indicators to an integrated, policy-relevant assessment of Europe's digital resilience.

References

Aryanti, D. R. (2025). Cybersecurity governance in public institutions: managing digital risks and resilience. *VISIONER: Jurnal Pemerintahan Daerah Di Indonesia*, 17(3), 24-35. <https://doi.org/10.54783/jv.v17i3.1424>

Ayeola, F. (2025) AI-Driven Anomaly Detection and Data Governance: Securing financial systems, cybersecurity networks, and regulatory compliance in multicultural ecosystems. *SSRN* <https://doi.org/10.2139/ssrn.5439102>

Brezavšček, A., & Baggia, A. (2025). Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. *Systems*, 13(1), 52. <https://doi.org/10.3390/systems13010052>

Brohi, S., Mastoi, Q.-U.-A., Jhanjhi, N. Z., & Pillai, T. R. (2025) A Research Landscape of Agentic AI and Large Language Models: Applications, Challenges and Future Directions. *Algorithms*, 18(8), 499. <https://doi.org/10.3390/a18080499>

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. *IEEE Access*, 10, 117814-117846. <https://doi.org/10.1109/ACCESS.2022.3204171>

Center for Security and Emerging Technology (CSET) (2024). Emerging technology and security: Policy recommendations. Georgetown University. <https://cset.georgetown.edu>

Dritsas, E., & Trigka, M. (2025). A Survey on Cybersecurity in the Internet of Things (IoT). *Future Internet*, 17(1), 30. <https://doi.org/10.3390/fi17010030>

ENISA. (2023). Cybersecurity by design for digital public services. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications>

Eom, S.-J., & Lee, J. (2022). Digital government transformation in turbulent times: Responses, challenges, and future direction. *Government Information Quarterly*, 39(3), <https://doi.org/10.1016/j.giq.2022.101690>

Gajdzik, B., Grabowska, S., & Saniuk, S. (2021). A theoretical framework for Industry 4.0 and its implementation with selected practical schedules. *Energies*, 14(4), 940. <https://doi.org/10.3390/en14040940>

Gianni, R., Lehtinen, S., & Nieminen, M. (2022). Governance of Responsible AI: From Ethical Guidelines to Cooperative Policies. *Front. Comput. Sci.*, 4, 873437. <https://doi.org/10.3389/fcomp.2022.873437>

Hazdiuk, K., Bilak, Y., Shumyliak, L., & Cibák, L. (2025). An experimental analysis of artificial intelligence (AI) use for traffic monitoring in urban environments. *Insights into Regional Development*, 7(4), 231-250. <https://doi.org/10.70132/n2454482348>

Haug, N., Dan, S., & Mergel, I. (2024). Digitally-induced change in the public sector: a systematic review and research agenda. *Public Management Review*, 26(7), 1963-1987. <https://doi.org/10.1080/14719037.2023.2234917>

Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025) A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*, 5, 314. <https://doi.org/10.1007/s44163-025-00578-1>

Huang, K., & Madnick, S.E. (2019) Does High Cybersecurity Capability Lead to Openness in Digital Trade? The Mediation Effect of E-Government Maturity within Cross-Border Digital Innovation. SSRN Working Paper 2019. <https://doi.org/10.2139/ssrn.3542552>

International Telecommunication Union (ITU). (2024). Global Cybersecurity Index (GCI) 2024. <https://www.itu.int>

Jarzębowski, S., Bozhenko, V., Didorenko, K., Tkachenko, O., Blyznyukov, A., Melnyk, M., & Cieslik, J. (2024). The Impact of Digitalisation on the Competitiveness of European Countries. *SocioEconomic Challenges*, 8(3), 238-261. [https://doi.org/10.61093/sec.8\(3\).238-261.2024](https://doi.org/10.61093/sec.8(3).238-261.2024)

Kamatchi, K., & Uma, E. (2025). Insights into User Behavioral-Based Insider Threat Detection: A Systematic Review. *Int. J. Inf. Sec.*, 24, 88. <https://doi.org/10.1007/s10207-025-01002-6>

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>

Kulothungan, V. (2025). Securing the AI Frontier: Urgent Ethical and Regulatory Imperatives for AI-Driven Cybersecurity. arXiv:2501.10467v1 <https://doi.org/10.48550/arXiv.2501.10467>

Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, 44(6), 101976. <https://doi.org/10.1016/j.telpol.2020.101976>

Mohammed, A., Goitia, D., Ahmad, S. A., & Ramlal, C. (2025). Revealing resilience: AI anomaly detection driven design considerations for Cyber Physical Systems supporting critical infrastructures in Small Island Developing States. *Insights into Regional Development*, 7(3), 148-169. <https://doi.org/10.70132/p6489444663>

Nott, C. (2025). Organisational Adaptation to Generative AI in Cybersecurity: A Systematic Review. arXiv 2025, preprint, arXiv:2506.12060. <https://doi.org/10.48550/arXiv.2506.12060>

Oxford Insights. (2024). Government AI Readiness Index 2024. Oxford Insights & International Development Research Centre. <https://govai.org>

Public Sector Network (n.d) <https://publicsectornetwork.com/>

Rjoub, G., Bentahar, J., Abdel Wahab, O., Mizouni, R., Song, A., Cohen, R., Otrok, H., & Mourad, A. (2023). A Survey on Explainable Artificial Intelligence for Cybersecurity. *IEEE Trans. Netw. Serv. Manag.*, 20(4), 5115-5140. <https://doi.org/10.1109/TNSM.2023.3282740>

Safitra, M.F., Lubis, M., & Fakhurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, 15, 13369. <https://doi.org/10.3390/su151813369>

Taddeo, M., Blanchard, A., & Thomas, C. (2024). From AI Ethics Principles to Practices: A Teleological Methodology to Apply AI Ethics Principles in the Defence Domain. *Philos. Technol.*, 37, 42. <https://doi.org/10.1007/s13347-024-00710-6>

Thakur, S. (2025). Policy, Governance, and Technology: What Drives AI Readiness? An Empirical Study of 155 Countries. SSRN. <https://doi.org/10.2139/ssrn.5233141>

Vatamanu, A.-F., & Tofan, M. (2025). Integrating artificial intelligence into public administration: Challenges and vulnerabilities. *Adm. Sci.*, 15(4), 149. <https://doi.org/10.3390/admsci15040149>

Vulpe, S.-N., Rughiniş, R., Țurcanu, D., & Rosner, D. (2024) AI and cybersecurity: a risk society perspective. *Front. Comput. Sci.*, 6, 1462250. <https://doi.org/10.3389/fcomp.2024.1462250>

Waara, Å. (2025). Examining Digital Government Maturity Models: Evaluating the Inclusion of Citizens. *Administrative Sciences*, 15(3), 73. <https://doi.org/10.3390/admsci15030073>

World Bank. (2022). GovTech Maturity Index 2022. World Bank Publications. <https://www.worldbank.org>

Zettl-Schabath, K., Bund, J., Müller, M., Borrett, C., Hemmelskamp, J., Alibegovic, A., Bajra, E., Jazxhi, A., Kellenter, E., Sachs, A., & Shelley, C. (2025) Global Dataset of Cyber Incidents (Version 1.3.2) [Data set]. European Repository of Cyber Incidents (EuRepoC), 2025. <https://eurepoc.eu/database/>

Data Availability Statement: All data used in this study are publicly available. The Digital Economy and Society Index (DESI) can be accessed through the European Commission’s digital public services portal. The Government AI Readiness Index data are available from Oxford Insights (2024). Cybersecurity capacity scores are retrieved from the ITU Global Cybersecurity Index (GCI 2024). Data on cyber incidents were obtained from the European Repository of Cyber Incidents (EuRepoC 2025). No new data were created by the authors.

Acknowledgments: No generative AI tools were used in the study design, data collection, analysis, interpretation, or writing of this manuscript.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Author Contributions: Conceptualisation, K.T. and I.B.; methodology, I.B.; software, L.C.; validation, I.B., J.M. and K.T.; formal analysis, K.T.; investigation, J.M.; resources, I.B.; data curation, L.C.; writing—original draft preparation, K.T.; writing—review and editing, I.B. and L.C.; visualisation, L.C.; supervision, I.B.; project administration, K.T.; funding acquisition, I.B.

Ivana Butoracová ŠINDLEROVÁ is a Professor at the Faculty of Social Sciences, University of Ss. Cyril and Methodius in Trnava, Slovakia. Research interests: Public administration, public policy, smart cities and regions, regional development, local government, strategic management in the public sector, digital transformation of public administration, innovation in public services, governance, and sustainable development.

ORCID: <https://orcid.org/0000-0001-8261-7490>

Lukáš CHUŤKA is a University Teacher and Researcher at the Faculty of Social Sciences, University of Ss. Cyril and Methodius in Trnava, Slovakia. Research interests: Information systems in public administration, digital governance, e-government, public sector innovation, information security, digital transformation, and information technologies in public institutions.

ORCID: <https://orcid.org/0009-0001-7353-9512>

Kamil TURČAN is a Researcher and University Teacher at the Faculty of Social Sciences, University of Ss. Cyril and Methodius in Trnava, Slovakia. Research interests: Public administration, regional development, smart cities, digital transformation in public administration, information systems management, project management in the public sector, innovation management, and sustainable development.

ORCID: <https://orcid.org/0000-0002-1236-0658>

Ján MACHYNIAK is an Associate Professor at the Faculty of Social Sciences, University of Ss. Cyril and Methodius in Trnava, Slovakia. Research interests: Political science, public policy, European politics, political systems, international relations, public administration, electoral studies, and contemporary political processes.

ORCID: <https://orcid.org/0000-0003-0747-0286>

Copyright © 2026 by author(s). Publishing rights by Entrepreneurship and Sustainability Center

This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>



Open Access