International Journal of Sustainable Development and Planning
Vol. 21, No. 9, September, 2026, pp. 4049-4058
Journal homepage: http://iieta.org/journals/ijsdp

Cybersecurity as a Foundation for Sustainable Digital Development: A Governance Framework for Emerging Economies

Blerton Abazi[1*], Nikola Protrka[2]

[1] Faculty of Information Systems, Computer Science and Engineering, University for Business and Technology (UBT), Prishtina 10000, Republic of Kosovo
[2] Police Academy, University of Applied Sciences in Criminal Investigation and Public Security, Zagreb 10000, Croatia

Corresponding Author Email: blerton.abazi@ubt-uni.net

Copyright: ©2026 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsdp.210909

Received: 9 July 2026
Revised: 16 September 2026
Accepted: 23 September 2026
Available online: 30 September 2026

Keywords:
cybersecurity governance, sustainable digital development, digital trust, emerging economies, European Union regulatory approximation, NIS2, Sustainable Development Goals 16, Kosovo

ABSTRACT

Digital transformation is increasingly positioned as a central pillar of sustainable development strategies in emerging economies, yet the cybersecurity foundations underpinning this transformation remain systematically underdeveloped. This paper argues that cybersecurity constitutes critical institutional infrastructure for sustainable digital development, directly conditioning progress toward Sustainable Development Goals 9 (resilient infrastructure), 11 (sustainable cities and communities) and 16 (peace, justice and strong institutions). Drawing on a structured qualitative document analysis of European Union regulatory instruments, including the NIS2 Directive, the Digital Operational Resilience Act (DORA), the Cyber Resilience Act and the Artificial Intelligence Act (AI Act), and of their diffusion into candidate and neighbourhood countries, the paper examines the governance gap between digitalization ambitions and cyber-resilience capacity in transition economies. It proposes a four-stage governance framework, Assess, Govern, Defend, Earn Trust, designed for resource-constrained institutional environments, in which risk assessment, regulatory alignment, operational defence and public digital trust operate as mutually reinforcing dimensions of sustainable digital governance. The framework is illustrated through the case of Kosovo, a candidate economy undergoing simultaneous digital transformation and European Union (EU) regulatory approximation, using sectoral evidence from financial services, public administration and higher education. The analysis suggests that fragmented, compliance-driven approaches accumulate a form of digital development debt that erodes the sustainability of digitalization gains, whereas trust-centred governance models generate durable institutional capacity. The paper contributes a transferable planning instrument for policymakers and argues for the formal integration of cyber-resilience indicators into national sustainable development planning frameworks.

1. INTRODUCTION

Digitalization has become a defining feature of contemporary development strategies. International organizations, development banks and national governments increasingly frame digital technologies as accelerators of the 2030 Agenda, capable of transforming public service delivery, expanding economic participation and improving the evidence base for planning decisions [1]. At the same time, a persistent lesson of development practice is that technology produces durable benefits only where complementary institutions, skills and regulation are in place; digital dividends do not accrue automatically, and their distribution depends on the analogue foundations that surround the technology [2]. Digital transformation is therefore best understood not as a technical migration but as a profound organizational and institutional change process [3].

Within this debate, one foundational condition has received comparatively little attention in the sustainable development and planning literature: cybersecurity. The expansion of e-government, digital finance, smart urban services and data-driven administration multiplies the attack surface of states and societies precisely in those contexts where protective capacity is weakest [4]. Cybersecurity has evolved from a narrow information-security concern into a societal issue that touches critical infrastructure, economic stability and the safety of citizens [5]. Global assessments consistently document a wide and persistent gap between the cybersecurity commitments of high-income countries and those of developing and transition economies [6]. For emerging economies, this gap is not merely a technical inconvenience; it is a structural vulnerability embedded in the core of their development model [7]. Cyber capacity building has consequently emerged as a field of international cooperation, though one still marked by fragmentation and asymmetries between donors and recipients [8].

This paper starts from a simple but consequential proposition: cybersecurity is institutional infrastructure for

sustainable digital development. Just as roads, grids and water systems underpin physical development, the confidentiality, integrity and availability of digital systems underpin the digital layer on which modern administration, commerce and civic life increasingly depend. Where that layer is fragile, digitalization gains are reversible: a major incident against a tax administration, a payment system or a hospital network can destroy in days the public trust that took years of investment to build. Conceived in this way, cybersecurity connects directly to three Sustainable Development Goals: SDG 9, which calls for resilient infrastructure; SDG 11, which requires safe and sustainable cities whose services are increasingly cyber-physical; and SDG 16, which demands effective, accountable and transparent institutions.

The paper pursues two research questions. RQ1: How does cybersecurity governance capacity condition the sustainability of digital development in emerging economies? RQ2: What governance model can integrate cyber-resilience into sustainable development planning under the resource and institutional constraints typical of transition contexts? To address these questions, the paper combines a review of scholarship at the intersection of digital government, cybersecurity governance and Europeanization with a qualitative document analysis of the current generation of European Union (EU) regulatory instruments and their diffusion into the enlargement region. On this basis it develops a four-stage governance framework, Assess, Govern, Defend, Earn Trust, and illustrates its application through the case of Kosovo, a candidate economy in which rapid digitalization, regulatory approximation and institutional consolidation are unfolding simultaneously.

The remainder of the paper is organized as follows. Section 2 reviews the relevant literature and identifies the research gap. Section 3 presents the research methodology. Section 4 characterizes the cyber-governance gap in emerging economies. Section 5 develops the proposed framework. Section 6 illustrates the framework through the Kosovo case. Section 7 discusses the findings, introduces the concept of digital development debt and draws policy implications. Section 8 concludes.

2. LITERATURE REVIEW

The argument of this paper sits at the intersection of three bodies of scholarship that have developed largely in isolation from one another: research on digital transformation and sustainable development; research on cybersecurity governance and institutions; and research on regulatory diffusion in EU candidate and neighborhood countries.

2.1 Digital transformation and sustainable development

A substantial literature examines how digital government evolves and under which conditions it contributes to development outcomes. Janowski [9] described digital government as an evolutionary process moving from digitization through transformation to contextualization, in which later stages depend on the institutional embedding of earlier ones. A recurring finding in this literature is the high failure rate of information-system initiatives in developing contexts, attributed to design-reality gaps between imported technological models and local institutional conditions [10]. More recent syntheses emphasize that information and communication technologies influence socioeconomic development through multiple, interacting channels, and that governance quality is a decisive moderator of their impact [11]. What remains largely implicit in this literature is the security dimension: digital services are typically treated as assets whose availability is assumed, rather than as contested infrastructures whose integrity must be actively defended [12]. Recent work in this journal on the adoption of strategic management tools likewise notes that digital integration and data security surface repeatedly as implementation challenges for organizations in transition economies, without yet being theorized as development constraints in their own right [13].

2.2 Cybersecurity governance and institutions

The cybersecurity literature has moved decisively beyond its technical origins. Cybersecurity is now widely conceptualized as an organizational and societal capability rather than a set of controls [5, 12], and its politics, who secures what, for whom and at what cost, has become an object of study in security studies and public policy [14]. Empirical work suggests that national cybersecurity capacity matters for outcomes: countries with more mature capacity experience measurably better results even after controlling for wealth and infrastructure penetration [15]. At the international level, cyber capacity building has become a recognized instrument of development cooperation, though scholars caution that it often reproduces donor priorities and struggles to generate locally owned institutions [8, 16]. Institutional theory offers a useful lens here: institutions, understood as the humanly devised constraints that structure interaction, determine whether formal rules translate into behavioural change [17], and technology enactment within public organizations is filtered through existing organizational arrangements rather than replacing them [18]. For emerging economies, the implication is that cybersecurity cannot be imported as a product; it must be grown as an institution.

2.3 Regulatory diffusion and Europeanization in accession contexts

For countries in the EU enlargement region, the reference model for cybersecurity governance is increasingly defined in Brussels. The Europeanization literature has long documented how conditionality and the transposition of the acquis reshape institutions in candidate countries, producing both genuine transformation and shallow, compliance-oriented adaptation [19, 20]. A rapidly growing body of scholarship examines the current generation of EU digital regulation as a distinct political and legal project. Farrand and Carrapico [21] interpreted the EU's turn toward assertive cybersecurity regulation as a shift from regulatory capitalism to regulatory mercantilism, in which security requirements become instruments of strategic autonomy; Bygrave [22] traced how EU cybersecurity law has emerged as a distinct, rapidly consolidating legal field; Vandezande [23] showed that the NIS2 Directive responds directly to the divergent and uneven transposition of its predecessor; and Kianpour et al. [24] demonstrated empirically that the directive most strongly operationalizes principles of governance authority, precisely the dimension weakest in transition administrations. This regulatory corpus, analysed in detail in Section 3, constitutes an unusually dense and prescriptive framework: the NIS2 Directive expands cybersecurity obligations across essential

and important sectors and strengthens supervisory and enforcement powers [D1]; the Digital Operational Resilience Act (DORA) harmonizes information and communication technology (ICT) risk management, incident reporting and third-party oversight in the financial sector [D2]; the Cyber Resilience Act introduces horizontal security requirements for products with digital elements [D3]; and the Artificial Intelligence Act (AI Act) establishes a risk-based regime for AI systems, including robustness and cybersecurity requirements for high-risk applications [D4]. Together with the General Data Protection Regulation (GDPR) [D5], these instruments define a de facto regulatory export that candidate countries progressively approximate. The literature, however, has examined this diffusion mainly through legal and administrative lenses; its consequences for the sustainability of digital development trajectories remain underexplored.

2.4 Research gap

Three gaps emerge from this review. First, the sustainable development and planning literature treats digitalization as an enabler while largely ignoring the security preconditions of that enabling role. Second, the cybersecurity governance literature is rich in national-level maturity assessment but thin on integration with development planning instruments, particularly for resource-constrained states. Third, the Europeanization literature analyses regulatory transfer without asking whether compliance-driven adoption produces resilient institutions or merely formal alignment. This paper addresses these gaps by conceptualizing cybersecurity as institutional infrastructure for sustainable digital development and by proposing a governance framework that connects cyber-resilience to SDG-oriented planning in emerging economies.

3. RESEARCH METHODOLOGY

The study adopts a qualitative, interpretive research design combining conceptual framework development with an illustrative single-case study [25]. This design is appropriate for the research questions, which concern how phenomena are connected, namely how cybersecurity governance conditions sustainable digital development, rather than how much, and for a field in which reliable quantitative indicators for the population of interest are scarce or, as discussed in Section 4, structurally absent for some territories.

3.1 Document corpus and analysis procedure

The research proceeded in three stages. In the first stage, a structured document analysis was conducted on two corpora. The first corpus comprises seven primary legal and regulatory instruments, listed in full in Appendix Table A and cited hereafter as [D1]-[D7]: five EU instruments, the NIS2 Directive [D1], the DORA [D2], the Cyber Resilience Act [D3], the AI Act [D4] and the GDPR [D5], and two Kosovo instruments used in the case analysis, the Law on Cyber Security [D6] and the Central Bank of the Republic of Kosovo Regulation on Information Systems and Cyber Risk Management [D7]. The second corpus comprises international assessment and policy documents relevant to emerging economies, including the International Telecommunication Union (ITU) Global Cybersecurity Index [6], the United Nations E-Government Survey [4], the European Union Agency for Cybersecurity (ENISA) Threat Landscape [26] and European Commission enlargement reporting for the Western Balkans [27].

The legal corpus was coded at the level of individual articles or article paragraphs of the operative text, following a two-cycle procedure adapted from qualitative content analysis; recitals and, with the exception of the Cyber Resilience Act's Annex I, annexes were excluded. In the first cycle, open coding of 89 provisions across [D1]-[D5] (35 in NIS2, 24 in DORA, 6 in the Cyber Resilience Act, 12 in the AI Act and 12 in the GDPR) generated 73 distinct provision-level codes describing discrete governance functions; examples include all-hazards risk management, management-body accountability, incident-notification deadlines, supply-chain security, management-training obligations and certification requirements, several of which recur across instruments (for instance, incident-notification deadlines are coded in NIS2 Article 23, DORA Article 19, the AI Act Article 73 and GDPR Article 33). In the second cycle, these codes were consolidated through constant comparison into six governance-function categories: (GF1) risk identification and assessment (9 provisions); (GF2) accountability and governance (15); (GF3) operational defence and incident response (25); (GF4) supply-chain and third-party oversight (11); (GF5) transparency, assurance and trust (20); and (GF6) capacity and resources (9). The codebook, with category definitions, example constituent codes, anchor provisions and boundary rules, is provided in Appendix Table B. Because the study is single-authored, inter-coder reliability could not be computed; consistency was instead addressed through an independent second coding pass on a purposive subsample of 28 provisions spanning the most control-dense parts of the corpus (NIS2 Article 21(2) and Article 23, DORA Articles 5-14 and GDPR Articles 25 and 32-35), conducted against the category definitions alone. Agreement between the two passes was 85.7% (24 of 28). The four disagreements concerned predictable boundary cases (asset management versus access control; post-incident learning versus plan revision; security-by-design versus trust safeguards; and breach notification to an authority versus to affected persons); each was resolved by adopting an explicit boundary rule, now recorded in Appendix Table B, after which the full corpus was checked against the final rules. A provision-level audit trail (coding workbook) is provided as supplementary material and referenced in the Data Availability statement.

In the second stage, the six governance-function categories identified in the document analysis were synthesized with the literature reviewed in Section 2 into a four-stage framework. The synthesis was guided by two design criteria derived from the institutional literature: parsimony, so that the framework can be operated by administrations with limited specialized staff, and cyclicality, so that the framework treats cyber-resilience as a continuous planning process rather than a one-off compliance exercise. The mapping is direct: GF1 grounds the Assess stage; GF2 and GF6 ground the Govern stage; GF3 and GF4 ground the Defend stage; and GF5 grounds the Earn Trust stage.

In the third stage, the framework was applied to the case of Kosovo. Kosovo was selected through purposive sampling as a revelatory case [25]: it combines rapid digitalization of public and financial services, active approximation of the EU acquis, acute human-resource constraints and, uniquely, exclusion from the principal international measurement systems, which makes the planning problem this paper

addresses visible in a particularly sharp form. The case analysis draws on publicly available regulatory and policy documents, including the Law on Cyber Security [D6], financial-sector regulation issued by the Central Bank of the Republic of Kosovo [D7] and European Commission country reporting [27], complemented by the author's professional observation of governance practice across the financial, public-administration and higher-education sectors, gathered through advisory and audit engagements conducted in accordance with professional confidentiality obligations. Throughout Section 6, claims that rest on this observational component rather than on citable documents are explicitly flagged as observational judgments, and Table 1 distinguishes documentary from observational evidence. This observational component is used strictly for illustration of the framework categories, not for hypothesis testing, and its limitations are acknowledged in Section 7.3.

Table 1. Mapping Kosovo's sectors against the framework (evidence basis per cell: Documentary sources cited; observational = author's professional observation, see Sections 3 and 7.3)

Sector	Regulatory Anchor	Observed Governance Pattern	Framework Stage Emphasis	Evidence Basis
Financial services	Central Bank of the Republic of Kosovo Regulation on Information Systems and Cyber Risk Management [D7]; supervisory expectations converging on the DORA model [D2]	Comparatively mature: mandated risk assessments, incident reporting to the supervisor, management-body accountability and independent review requirements [D7]; growing use of crisis simulations and structured board training (observational)	Strong Assess and Govern; maturing Defend; Earn Trust emerging through supervisory transparency	Documentary [D7, D2] + observational
Public administration	Law No. 08/L-173 on Cyber Security (2023) [D6]; national cybersecurity strategy; approximation commitments under the European Union (EU) accession process [27]	Institutionally young: new competent authority and CSIRT functions being consolidated [27]; uneven implementation across institutions and limited administrative capacity [27]; dependency on donor-funded projects and scarce specialized staff (observational)	Govern formally advanced; Assess and Defend under-resourced; Earn Trust largely unaddressed	Documentary [D6, 27] + observational
Higher education	Institutional autonomy; accreditation requirements; no dedicated sectoral cybersecurity regime	Dual role as vulnerable operator and capacity producer: growing cybersecurity curricula and certification pathways; institutional security practices variable; strategic workforce role recognized but not planned (observational)	Critical to Govern (workforce) and Earn Trust (skills, awareness); own Defend posture weak	Observational

4. THE CYBER-GOVERNANCE GAP IN EMERGING ECONOMIES

Two global measurement systems frame the empirical starting point of this paper. The United Nations E-Government Survey tracks the supply of digital government through the E-Government Development Index and documents sustained growth in online service provision across all income groups [4]. The ITU Global Cybersecurity Index measures national cybersecurity commitments across legal, technical, organizational, capacity-development and cooperation pillars, and consistently finds that mature, whole-of-government cybersecurity postures are concentrated in high-income countries, while a large group of developing and transition economies remains at basic or evolving stages [6]. Read together, the two instruments describe a structural asymmetry: the digital attack surface of emerging economies is expanding faster than their protective capacity.

Threat conditions amplify this asymmetry. European threat reporting documents the industrialization of ransomware, the growth of supply-chain compromises and the increasing targeting of public administration, health, energy and finance, precisely the sectors that anchor development strategies [26]. Emerging economies face these threats with thinner defensive labour markets, smaller security budgets and, critically, weaker institutional mechanisms for translating incidents into learning. The result is a governance gap with four recurrent features. First, strategy-implementation decoupling: national cybersecurity strategies are adopted, often with donor support, but lack the budgeted action plans, staffing and enforcement mechanisms required to change organizational behaviour [16]. Second, regulatory borrowing without institutional grounding: legal texts closely modelled on EU instruments are transposed while the supervisory authorities, computer security incident response teams and audit functions they presuppose remain embryonic [19, 20]. Third, sectoral unevenness: internationally exposed sectors such as banking, disciplined by correspondent relationships and supervisory expectations, develop substantially stronger practices than general public administration, creating resilience islands in a fragile institutional sea. Fourth, measurement invisibility: for some territories, non-membership in international organizations excludes them from the very indices through which the gap is monitored, leaving planners without external benchmarks.

The fourth feature deserves emphasis because it converts a data problem into a planning problem. A state that appears in neither the E-Government Development Index nor the Global Cybersecurity Index cannot anchor its digital development targets to recognized international baselines, cannot demonstrate progress to investors and partners through standard instruments, and is structurally at risk of underinvesting in capabilities that are never externally scored. Kosovo, examined in Section 6, is the paradigmatic case. For such contexts, a governance framework must be operable from domestic evidence and must itself generate the indicators that international systems do not supply.

5. THE ASSESS-GOVERN-DEFEND-EARN TRUST FRAMEWORK

This section develops the paper's central contribution: a four-stage governance framework that integrates cyber-resilience into sustainable digital development planning. The framework, shown in Figure 1, is deliberately parsimonious. It compresses the governance functions (GF1-GF6, Appendix Table B) prescribed by the EU regulatory corpus and recommended by capacity-building practice into four stages, Assess, Govern, Defend and Earn Trust, arranged as a continuous cycle around the objective of sustainable digital development. The cycle closes through a feedback loop from trust outcomes back into assessment, reflecting the premise that resilience is a process property of institutions, not a state achieved once. Table 2 summarizes the stages, their core functions, characteristic instruments and primary SDG linkages.

5.1 Assess: Evidence before architecture

The first stage establishes the evidence base on which all subsequent governance choices depend. It comprises the identification of critical services and their digital dependencies, structured risk assessment, maturity benchmarking and continuous monitoring of the threat landscape. In mature regulatory systems this function is institutionalized: the NIS2 Directive obliges essential and important entities to adopt risk-management measures grounded in an all-hazards analysis [D1], and DORA requires financial entities to maintain a comprehensive ICT risk-management framework as a precondition for everything else the regulation demands [D2]. For emerging economies the stage has an additional, compensatory role identified in Section 4: where international indices do not reach, domestically generated assessment evidence must substitute for external benchmarks. Practically, this argues for lightweight national instruments, a register of critical information infrastructure, a recurring public-sector maturity self-assessment and a national vulnerability-assessment programme, whose results feed directly into development planning documents rather than remaining confined to security institutions.

5.2 Govern: Institutions before controls

The second stage translates evidence into institutional arrangements: laws and secondary regulation, designated competent authorities, allocation of accountability within organizations and, critically, resourcing. The design principle here is proportionate approximation. The EU corpus offers candidate countries a coherent regulatory model, but wholesale transposition without regard to administrative capacity reproduces the shallow Europeanization documented in the enlargement literature [19, 20]. Proportionate approximation instead sequences obligations, prioritizing the governance spine, a competent authority with real supervisory powers, management-level accountability duties modelled on Article 20 of NIS2 [D1], and a functioning national Computer Security Incident Response Team (CSIRT), before extending sectoral coverage. The stage also encompasses the workforce dimension: governance arrangements that presuppose specialists who do not exist in the local labour market are decorative. Emerging economies therefore need explicit cybersecurity workforce strategies linking higher education, professional certification and public-sector retention, a point developed in the Kosovo case.

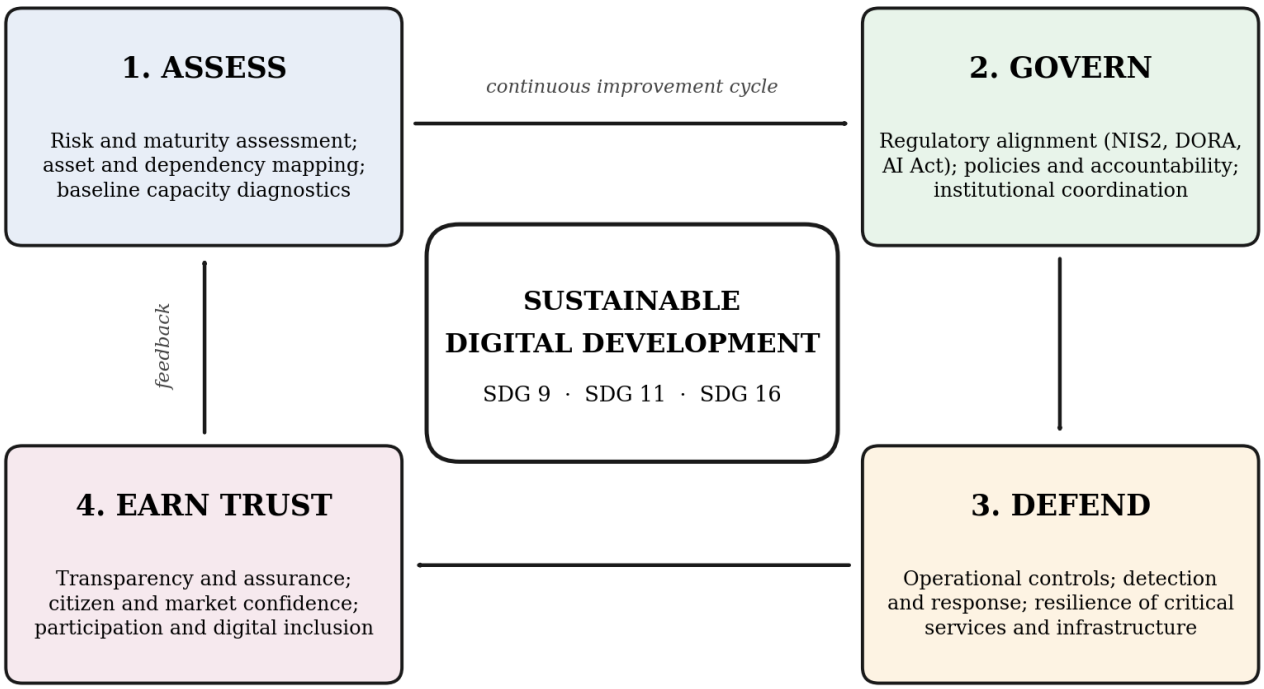


Figure 1. The Assess-Govern-Defend-Earn Trust governance framework for sustainable digital development

5.3 Defend: Resilience of what matters

The third stage concerns operational protection: preventive and detective controls, incident response, crisis management and continuity of critical services, including the cyber-physical services, energy, water, transport, health, that constitute the material substance of SDG 11. Two emphases distinguish the framework's treatment of this stage from

conventional control catalogues. The first is selectivity: under resource constraints, defence must concentrate on the services whose disruption would most damage development outcomes, as identified in the Assess stage, rather than distributing thin controls uniformly. The second is exercised capability: incident-response plans that have never been rehearsed fail under pressure, and therefore regular crisis exercises, including at the executive and board level, are treated as first-order governance instruments rather than training luxuries. Baseline control frameworks such as ISO/IEC 27001 provide a common vocabulary, but the framework treats certification as an instrument of the Defend stage, not as its objective.

5.4 Earn Trust: The sustainability test

The fourth stage is the framework's distinctive element and the point at which cybersecurity connects most directly to sustainability. Digital development is sustainable only if citizens, firms and international partners are willing to keep using, and investing in, digital systems; that willingness is a stock of trust that security incidents, opaque data practices and unaccountable automation steadily deplete. The Earn Trust stage therefore assembles the outward-facing governance functions: transparent breach notification and public communication; independent audit and assurance over public digital systems; data-protection governance aligned with the GDPR model [D5]; participatory oversight of algorithmic and AI systems consistent with the risk-based logic of the AI Act [D4]; and sustained investment in digital skills and awareness, which convert citizens from the weakest link into a distributed sensor network. Trust outcomes, measured through service uptake, incident-reporting behaviour and survey instruments, feed back into the Assess stage, closing the cycle. In this design, trust is not a public-relations by-product of security; it is the criterion against which the sustainability of the whole digital development trajectory is evaluated, echoing the institutional emphasis of SDG 16.

6. CASE ILLUSTRATION: KOSOVO

Kosovo offers a revelatory setting in which the framework's categories become unusually visible. It is among Europe's youngest states and youngest populations, has digitalized public services rapidly through the central e-Kosova platform, and has been granted EU candidate perspective, with the Commission's 2024 enlargement reporting recording both progress in digital policy and persistent gaps in cybersecurity implementation capacity [27]. At the same time, because Kosovo is not a member of the United Nations or the ITU, it appears in neither the E-Government Development Index nor the Global Cybersecurity Index: the measurement invisibility described in Section 4 in its purest form. Development planning must therefore run on domestic evidence, which is precisely the situation the proposed framework is designed for. Consistent with Section 3, sector-level characterizations below are supported by cited documents where these exist; statements resting on the author's professional observation are explicitly marked as observational judgments, and Table 2 records the evidence basis of each characterization.

Table 2. The four stages of the framework: Functions, instruments and Sustainable Development Goals (SDG) linkages

Stage	Core Governance Functions	Key Instruments and Mechanisms	Primary SDG Linkage
Assess	Identification of critical services, assets and dependencies; risk and maturity assessment; threat-landscape monitoring; baseline capacity diagnostics	National risk assessments; sectoral maturity models; asset and dependency registers; vulnerability assessment and audit programmes	SDG 9.1, 9.a (resilient infrastructure); SDG 11.b (risk-informed planning)
Govern	Regulatory alignment and proportionate transposition; allocation of accountability; inter-institutional coordination; resourcing and workforce planning	Cybersecurity law and secondary regulation aligned with NIS2/DORA; designated competent authority; management accountability duties; sectoral supervision	SDG 16.6 (effective, accountable institutions); SDG 16.a (institutional capacity)
Defend	Preventive and detective controls; incident response and crisis management; resilience of critical and cyber-physical urban services; supply-chain security	National and sectoral Computer Security Incident Response Teams (CSIRTs); incident-reporting regimes; business continuity and crisis exercises; baseline control frameworks (e.g., ISO/IEC 27001)	SDG 9.1 (reliable infrastructure); SDG 11.5 (reduced disruption losses)
Earn Trust	Transparency and assurance towards citizens and markets; data protection; digital inclusion and skills; participatory oversight of AI and data use	Independent audit and certification; breach notification and public communication; privacy governance; awareness and education programmes	SDG 16.6, 16.10 (transparency, access to information); SDG 4.4 (digital skills)

6.1 Financial services: A resilience island

The financial sector illustrates how external discipline accelerates the cycle. Banks and microfinance institutions operate under the Central Bank of the Republic of Kosovo Regulation on Information Systems and Cyber Risk Management [D7], approved in August 2025 with a transition period requiring full compliance with its mandatory standards by 1 June 2026. The regulation mandates an ICT and cyber risk-management framework, allocates explicit responsibilities to management bodies, and scales obligations to the size, risk profile and complexity of each institution; at the time of writing, the sector is therefore inside a supervised transition window in which the framework's Assess-Govern-Defend cycle can be observed operating in real time. Institutions also maintain correspondent relationships that

impose international expectations and are examined by a supervisor whose requirements increasingly converge on the DORA model [D2, 28]. In consequence, the sector exhibits the strongest Assess and Govern practice in the country: mandated risk assessments, management-body accountability for ICT risk, incident-reporting obligations and independent review [D7]. As an observational judgment grounded in the author's advisory engagements, defend capability is maturing, with institutions progressively adopting structured crisis simulations and board-level cybersecurity training as exercised, rather than merely documented, capabilities. The sector demonstrates the framework's cyclical logic in miniature: supervisory assessment findings drive governance adjustments, which fund defensive investment, which is communicated to the supervisor and the market, sustaining the trust on which a small, euroized financial system critically depends.

6.2 Public administration: Governance ahead of capacity

Public administration displays the inverse pattern: formal governance running ahead of operational capacity. The 2023 Law on Cyber Security transposes core elements of the EU model, establishing a competent authority, incident-reporting duties and critical-infrastructure identification [D6]. On paper, the Govern stage is substantially complete. In practice, implementation confronts constraints documented in the Commission's 2024 country reporting, which records that the new institutional framework remains in early consolidation and that administrative capacity for implementation is limited [27], together with features typical of the region: a thin specialized labour market in which public salaries cannot compete with private and international demand, and dependence on donor-funded projects whose timelines rarely match institutional absorption (observational judgments). A further observational judgment, offered as such, is that security practice remains uneven across the dozens of institutions connected to shared platforms, so that the weakest institution effectively defines the exposure of the whole. In framework terms, Assess is fragmentary, Defend is concentrated in a small number of central functions, and Earn Trust has not yet been articulated as a policy objective at all, despite the fact that citizen uptake of e-services is the declared purpose of the digital agenda. The case illustrates the paper's central warning: transposition without institutional grounding accumulates digital development debt.

6.3 Higher education: The workforce hinge

Higher education occupies a dual position in the framework. As operators of research and student-data systems, universities are themselves targets, and as an observational judgment their Defend posture is generally weak. As producers of the cybersecurity workforce, however, they are the hinge on which the national Govern stage turns: no governance arrangement in Sections 6.1 and 6.2 is sustainable without a domestic supply of qualified professionals. Kosovar institutions have begun building dedicated cybersecurity curricula, professional certification pathways and applied training, including board-level and awareness formats delivered to industry, but this supply function is not yet integrated into national planning: there is no workforce gap analysis linking projected regulatory demand, driven by the new law's coverage [D6], to enrolment and curriculum policy. The framework makes this linkage explicit by locating workforce development within the Govern stage and skills diffusion within Earn Trust, converting an educational question into a development-planning one.

7. DISCUSSION

7.1 Digital development debt

The analysis motivates a concept that names the central risk facing digitalizing emerging economies: digital development debt. By analogy with technical debt in software engineering, digital development debt is the accumulated gap between the pace at which a polity digitalizes its critical functions and the pace at which it builds the assessment, governance, defensive and trust-maintaining capacity that digitalization presupposes. Like financial debt, it is invisible while conditions are benign and is called in at the worst moment: a successful attack against a core registry, payment system or municipal service does not merely impose recovery costs, it liquidates trust, suppresses service uptake and can reverse years of development gains. The Kosovo public-administration case shows how the debt accumulates through the most well-intentioned channel, rapid legal approximation, when transposition outruns institutional absorption. The framework's cyclical design is, in essence, a debt-management instrument: each pass through Assess-Govern-Defend-Earn Trust amortizes accumulated exposure and prevents new borrowing against institutional capacity that does not exist.

7.2 Policy implications

Four implications follow for policymakers and planners in emerging economies. First, cyber-resilience indicators should be integrated formally into national sustainable development planning frameworks, alongside conventional infrastructure and governance indicators, so that security investment competes for resources as development spending rather than as discretionary IT expenditure. Second, regulatory approximation should be sequenced by governance function rather than by legal instrument: the supervisory spine and accountability duties first, comprehensive sectoral coverage later, accepting slower formal alignment in exchange for real institutional depth. Third, sectoral asymmetries should be exploited deliberately: mature sectors such as finance can serve as capability exporters to public administration through structured secondments, shared exercises and common assurance services, rather than remaining isolated resilience islands. Fourth, for territories excluded from international measurement systems, governments should institutionalize domestic assessment instruments whose methodology mirrors the international indices, generating comparable evidence for planning and for external partners, and should treat this evidence-generation capacity itself as development infrastructure.

7.3 Limitations

Three limitations bound the contribution. First, the framework is derived conceptually from regulatory analysis and literature synthesis; it has not been validated through comparative empirical testing, and its stage boundaries are analytical conveniences that overlap in practice. Second, the

case illustration rests on a single territory and incorporates the author's professional observation, which, while grounded in sustained sectoral engagement and now explicitly flagged wherever it is relied upon (Section 6, Table 2), is subject to selection and confirmation biases inherent to participant observation; the associated conflict-of-interest considerations are declared in the statements below. Third, the argument generalizes most safely to EU candidate and neighbourhood countries, for which the European regulatory model is the operative reference; its transfer to emerging economies in other regulatory orbits requires adaptation that this paper does not undertake. Future research should operationalize the framework's stages into measurable indicators, test the digital development debt proposition against incident and service-uptake data across a panel of transition economies, and examine comparatively whether trust-centred governance models outperform compliance-centred ones in sustaining digitalization gains.

8. CONCLUSIONS

This paper has argued that cybersecurity is not a technical overhead of digitalization but institutional infrastructure for sustainable digital development, conditioning progress toward SDGs 9, 11 and 16 in the same way that physical infrastructure conditions conventional development. Reviewing the intersection of digital government, cybersecurity governance and Europeanization scholarship, and analysing the current EU regulatory corpus and its diffusion into the enlargement region, the paper identified a recurrent governance gap in emerging economies, characterized by strategy-implementation decoupling, regulatory borrowing without institutional grounding, sectoral unevenness and, for some territories, exclusion from international measurement systems. In response, the paper proposed the Assess-Govern-Defend-Earn Trust framework: a parsimonious, cyclical governance model that integrates risk assessment, proportionate regulatory alignment, selective operational defence and the active maintenance of public digital trust into a single planning instrument operable under resource constraints. The Kosovo case illustrated the framework's diagnostic power, revealing a financial sector functioning as a resilience island, a public administration whose formal governance runs ahead of operational capacity, and a higher-education sector whose workforce role is the unplanned hinge of the whole system. The concept of digital development debt was introduced to name the risk that transposition-led digitalization accumulates: invisible in calm conditions, ruinous when called.

The practical recommendation to planners is direct: treat cyber-resilience as a line item of sustainable development, sequence governance before coverage, mobilize mature sectors as capability exporters, and where international indices do not reach, build the domestic evidence machinery that makes disciplined planning possible. Digitalization will remain central to the development strategies of emerging economies; whether its gains prove durable will depend less on the technologies adopted than on the trustworthiness of the institutions that govern them.

CONFLICT OF INTEREST

The author declares no conflict of interest. Although the case observations are informed by the author's professional advisory and audit experience, these roles did not influence the conduct, analysis, or reporting of the research.

ETHICS STATEMENT

This study is based on the analysis of publicly available legal, regulatory and policy documents and on the author's professional observation at sector level. No human participants were recruited, no interviews were conducted, and no personal or client-confidential data were collected or processed; accordingly, ethics committee approval was not required. Observational statements are reported only at an aggregated, sector level and in compliance with the professional confidentiality obligations attached to the underlying engagements.

DATA AVAILABILITY

All documents analysed in this study are publicly available from the official sources listed in Appendix A and in the reference list. The provision-level coding audit trail (workbook containing the codebook, the 89 coded provisions with first-cycle codes and category assignments, and the consistency-check subsample with agreement calculation) is provided as supplementary material and is also available from the corresponding author. No further datasets were generated or analysed.

REFERENCES

[1] Sachs, J.D., Schmidt-Traub, G., Mazzucato, M., Messner, D., Nakicenovic, N., Rockstrom, J. (2019). Six transformations to achieve the Sustainable Development Goals. Nature Sustainability, 2: 805-814. https://doi.org/10.1038/s41893-019-0352-9

[2] World Bank. (2016). World development report 2016: Digital dividends. Washington, DC: World Bank. https://doi.org/10.1596/978-1-4648-0671-1

[3] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2): 118-144. https://doi.org/10.1016/j.jsis.2019.01.003

[4] United Nations Department of Economic and Social Affairs. (2024). E-government survey 2024: Accelerating digital transformation for sustainable development. New York: United Nations.

[5] von Solms, R., van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38: 97-102. https://doi.org/10.1016/j.cose.2013.04.004

[6] International Telecommunication Union. (2024). Global cybersecurity index 2024. Geneva: ITU Publications. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.

[7] Kshetri, N. (2013). Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan London. https://doi.org/10.1057/9781137021946

[8] Calderaro, A., Craig, A.J.S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. Third World Quarterly, 41(6): 917-938. https://doi.org/10.1080/01436597.2020.1729729

[9] Janowski, T. (2015). Digital government evolution: From transformation to contextualization. Government Information Quarterly, 32(3): 221-236. https://doi.org/10.1016/j.giq.2015.07.001
[10] Heeks, R. (2002). Information systems and developing countries: Failure, success, and local improvisations. The Information Society, 18(2): 101-112. https://doi.org/10.1080/01972240290075039
[11] Roztocki, N., Soja, P., Weistroffer, H.R. (2019). The role of information and communication technologies in socioeconomic development: Towards a multi-dimensional framework. Information Technology for Development, 25(2): 171-183. https://doi.org/10.1080/02681102.2019.1596654
[12] Craigen, D., Diakun-Thibault, N., Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10): 13-21. https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf.
[13] Lubeniqi, G., Zefaj, E., Avdimetaj, K. (2026). Application of strategic management tools and techniques by small and medium-sized enterprises: A qualitative review. International Journal of Sustainable Development and Planning, 21(2): 859-868. https://doi.org/10.18280/ijsdp.210234
[14] Dunn Cavelty, M., Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1): 5-32. https://doi.org/10.1080/13523260.2019.1678855
[15] Dutton, W.H., Creese, S., Shillair, R., Bada, M. (2019). Cybersecurity capacity: Does it matter? Journal of Information Policy, 9: 280-306. https://doi.org/10.5325/jinfopoli.9.2019.0280
[16] Pawlak, P., Barmpaliou, P.N. (2017). Politics of cybersecurity capacity building: Conundrum and opportunity. Journal of Cyber Policy, 2(1): 123-144. https://doi.org/10.1080/23738871.2017.1294610
[17] North, D.C. (1990). Institutions, Institutional Change and Economic Performance. Cambridge: Cambridge University Press.
[18] Fountain, J.E. (2001). Building the Virtual State: Information Technology and Institutional Change. Washington, DC: Brookings Institution Press.
[19] Grabbe, H. (2006). The EU's Transformative Power: Europeanization through Conditionality in Central and Eastern Europe. Palgrave Macmillan London. https://doi.org/10.1057/9780230510302
[20] Borzel, T.A., Risse, T. (2012). From Europeanisation to diffusion: Introduction. West European Politics, 35(1): 1-19. https://doi.org/10.1080/01402382.2012.631310
[21] Farrand, B., Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. European Security, 31(3): 435-453. https://doi.org/10.1080/09662839.2022.2102896
[22] Bygrave, L.A. (2025). The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. Computer Law & Security Review, 56: 106071. https://doi.org/10.1016/j.clsr.2024.106071
[23] Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, 52: 105890. https://doi.org/10.1016/j.clsr.2023.105890
[24] Kianpour, M., Earls Davis, P.A., Windekilde, I.M. (2025). Digital sovereignty in practice: Analyzing the EU's NIS2 directive. International Journal of Information Security, 24: 167. https://doi.org/10.1007/s10207-025-01090-4
[25] Yin, R.K. (2018). Case Study Research and Applications: Design and Methods, 6th ed. Thousand Oaks: Sage Publications.
[26] European Union Agency for Cybersecurity (ENISA). (2024). ENISA threat landscape 2024. Athens: ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[27] European Commission. (2024). Kosovo 2024 Report. Commission Staff Working Document, SWD(2024) 692 final, Brussels, 30.10.2024. Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024SC0692.
[28] Ismaili, A. (2023). Cybersecurity in the banking industry. Governor of the Central Bank of the Republic of Kosovo. https://www.bis.org/speeches/20231114-cybersecurity-banking-industry.pdf.

APPENDIX

Table A. Document corpus

No.	Issuing Body	Year	Title of Instrument	Official Source
Doc. 1	European Parliament and Council	2022	Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)	Official Journal of the European Union
Doc. 2	European Parliament and Council	2022	Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA)	Official Journal of the European Union
Doc. 3	European Parliament and Council	2024	Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)	Official Journal of the European Union
Doc. 4	European Parliament and Council	2024	Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)	Official Journal of the European Union
Doc. 5	European Parliament and Council	2016	Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation (GDPR))	Official Journal of the European Union
Doc. 6	Assembly of the Republic of Kosovo	2023	Law No. 08/L-173 on Cyber Security	Official Gazette of the Republic of Kosovo
Doc. 7	Central Bank of the Republic of Kosovo	2025	Regulation on Information Systems and Cyber Risk Management, approved August 2025 (full compliance required by 1 June 2026)	Prishtina: Central Bank of the Republic of Kosovo

Table B presents the six governance-function categories produced by the second coding cycle (Section 3.1), their definitions, examples of the 73 first-cycle constituent codes, illustrative anchor provisions in the corpus, and the five boundary rules adopted after the consistency check. The provision-level audit trail (89 coded provisions) is provided as supplementary material (see Data Availability).

Table B. Governance-function categories, constituent codes and anchor provisions

Category	Definition	Example Constituent Codes (of 73)	Anchor Provisions
GF1 Risk identification and assessment	Obligations to identify critical services, assets and dependencies and to assess risks on an all-hazards basis	all-hazards risk management; risk-analysis policies; asset and dependency identification; incident classification; control-effectiveness assessment; impact assessment	[D1] Arts. 21(1), 21(2)(a), 21(2)(f); [D2] Arts. 6, 8, 18; [D4] Arts. 9-10; [D5] Art. 35
GF2 Accountability and governance	Allocation of responsibility to management bodies, competent authorities and supervisors	management-body accountability; competent-authority designation; supervision and enforcement powers; sanctions; proportionality; inter-institutional coordination	[D1] Arts. 8, 14, 20(1), 27, 31-35; [D2] Arts. 5, 16, 46-50; [D3] Art. 52; [D4] Arts. 17, 70; [D5] Arts. 24, 37, 58, 83
GF3 Operational defence and incident response	Preventive and detective controls, incident handling, notification and continuity of operations	incident handling; notification to authorities (NIS2, DORA, AI Act, GDPR); business continuity; backup and recovery; resilience and penetration testing; security-by-design controls	[D1] Arts. 21, 23; [D2] Arts. 9-12, 17-19, 24-26; [D5] Arts. 25, 32-33
GF4 Supply-chain and third-party oversight	Security of supplier relationships, third-party ICT services and products with digital elements	supply-chain security; supplier risk evaluation; third-party ICT risk register; concentration risk; contractual requirements; critical-provider oversight; product security-by-design	[D1] Arts. 21(2)(d), 21(3), 22; [D2] Arts. 28-33; [D3] Arts. 13, Annex I; [D5] Art. 28
GF5 Transparency, assurance and trust	Outward-facing obligations that sustain the confidence of users, markets and data subjects	notification to users, clients and data subjects; certification and conformity assessment; standards; documentation and record-keeping; human oversight; information sharing; privacy principles	[D1] Arts. 12, 23(1), 24-25, 29; [D2] Arts. 14, 19(3), 45; [D3] Arts. 28-30; [D4] Arts. 11-14, 50; [D5] Arts. 30, 34, 42
GF6 Capacity and resources	Requirements and enablers concerning skills, staffing, funding and institutional capabilities	management-training obligations; cyber hygiene and training; CSIRT establishment and capabilities; awareness and learning; strategy content; AI literacy	[D1] Arts. 7, 10-11, 20(2), 21(2)(g); [D2] Arts. 5(4), 13; [D4] Art. 4

Boundary rules adopted after the consistency check: (1) notification to a public authority is coded GF3, notification to users, clients or data subjects GF5; (2) identification or inventory of assets and dependencies is GF1, access-control and asset-handling controls GF3; (3) security-by-design obligations on controllers and operators are GF3, certification, documentation and conformity assessment GF5; (4) post-incident learning is GF6 when framed as awareness or training and GF3 when framed as plan revision; (5) third-party and processor contractual requirements are GF4 in every instrument.