information, and critical educational workflows. Recent analyses highlight the persistence of threats to the sector such as phishing, malware, credential compromise, software vulnerabilities, poor incident reporting and a low level of cybersecurity awareness (Afolalu & Tsoeu, 2025; Salam et al., 2026). Cybersecurity in universities is therefore not merely a technical infrastructure to be managed: the resilience of an institution depends as much on its governance arrangements — organisational capability, internal regulation, staff practice, and coordination between those responsible — as on the security of its critical technical infrastructure.

In this, the Ukrainian case is no exception. Under martial law, universities continue to function in the face of cyberattack, disinformation, the threat of personal data leaks, and a growing dependence on digital communication and distance education services (Chornomydz, 2025). At national level, the Cybersecurity Strategy of Ukraine identifies cyber resilience, institutional cooperation, capacity building, and a secure national cyberspace as areas of strategic importance (President of Ukraine, 2021). These priorities have not yet been translated adequately into the means by which the higher education sector itself is governed.

Current cybersecurity policy is converging on the treatment of cybersecurity as a public-governance challenge that can be addressed only through the coordinated application of informational, regulatory, financial and organisational instruments, rather than through stand-alone technical tools (Cotta & Righettini, 2026). The higher education literature, by contrast, continues to be concerned primarily with threats, vulnerabilities, awareness, and technical safeguards (Afolalu & Tsoeu, 2025; Salam et al., 2026). There is therefore a disconnect between national-level cybersecurity governance and the level of the Ukrainian university.

This study asks how legal rules and institutional governance can support cybersecurity as a medium of sustainable digital transformation in Ukrainian higher education. It is guided by three questions: how national cybersecurity priorities are realised at the level of the university; what type of institutional arrangements enhance cyber resilience; and in which areas of public governance such capacity is lacking.

The question is posed here as a legal and institutional one rather than a technical one. What is at issue is not which controls a university should deploy, but how a binding national cybersecurity regime and a statutorily autonomous university are to be connected: which obligations attach to a higher education institution as a regulated organisation, which follow instead from its own governing decisions, and through what interface the two meet. Framed in these terms, the analysis belongs to the study of law, digital technologies and sustainable governance, and it is offered as a contribution to that field.

2. Literature Review

Studies of cybersecurity in higher education are converging on the view that universities are not simply another kind of digitally intensive organisation but a distinctive security environment. Their openness, diverse user bases, decentralised decision-making, large data holdings, and reliance on interconnected academic and administrative systems make

traditional information-security paradigms difficult to apply. Bongiovanni (2019) pointed out that information security management in higher education is a field that has attracted little research attention, particularly as regards security culture, cross-institutional studies, and security economics. Subsequent reviews have broadened the evidential basis but have not substantially addressed this deficit in governance. One such review (2022) highlighted increasing academic and administrative information risk in step with greater reliance on cloud services, while Nuñez et al. (2023) classified organisational responses as institutional, technological, physical, and standards-based security measures. The strength of these analyses is that they identify operational vulnerabilities and the controls available against them; what is missing is an account of institutional security as part of, rather than distinct from, a broader public-governance regime.

The same tendency appears in research on information security frameworks. Merchan--Lima et al. (2021) found a wide variety of frameworks, implementation phases, infrastructure services, and protective mechanisms in use across higher education institutions. This shows that cybersecurity is not simply a matter of deploying individual technical controls. However, this diversity of frameworks also poses a challenge to institutional consistency: the presence of standards does not by itself determine who is responsible, how priorities are coordinated, or how compliance and accountability are ensured among multiple actors. The ISO 27000-series standards and the CIS controls are examples of frameworks used by universities (Nuñez et al., 2023), but these instruments are designed principally to define security practices, not to allocate authority in the public sector. As a result, the literature is better equipped to answer how a university information system can be protected than how responsibility for cybersecurity should be governed.

This article approaches the emergent scholarship on cyber-governance from a wider conceptual vantage point. Kuerbis and Badiei (2017) distinguish market, networked, and hierarchical governance mechanisms, and show that cybersecurity is the outcome of the interaction of these mechanisms rather than of government hierarchy alone. Correspondingly, Savaş and Karataş (2022) argue that management without stakeholder-inclusive cyber governance is insufficient, and observe that no universally accepted governance model exists. Recent evidence cements this institutional reading. Carmichael (2026), analysing Estonia through the lens of collaborative governance, demonstrates that responsibility for cybersecurity within government can shift over time, and that conceptions of cybersecurity may remain underdeveloped even in a digitally mature state. Collectively, these works challenge state-centric models, but their level of analysis remains overwhelmingly national or ecosystem-wide. They offer a useful vocabulary for analysing coordination and responsibility, but they do not specify how such arrangements should operate in a field marked by university autonomy, public regulation, academic openness and decentralised digital infrastructure.

The gap is more pronounced in the digital-transformation literature. Castro Benavides et al. (2020) found that no genuinely holistic models of digital transformation exist for the higher education context. Fernández et al. (2023) show that digital transformation involves strategic, informational, process, technological, and human change rather than technology implementation alone. Their review of university projects indicates considerable attention to the quality of education, but also questions whether such isolated projects have a place

within an overall institutional digital strategy. Farias-Gaytan et al. (2023) similarly show that research focuses overwhelmingly on digital competences and educational technologies, with some attention to broader aspects of digital literacy. The transformation literature therefore acknowledges institutional complexity, but it does not often conceptualise cybersecurity governance as a component of the digital transformation process.

This tension is further highlighted by studies of barriers. Gkrimpizi et al. (2023) identify twenty barriers, grouped into environmental, strategic, organisational, technological, people-related and cultural categories, and conclude that the technical capability of an organisation is not the only reason why digital transformation fails. Singun (2025) extends this view through nine dimensions: digital vision, leadership, organisation, resources, competence, stakeholder management, culture, academic processes and ethics. These multidimensional approaches are analytically valuable because they move beyond technological determinism. However, cybersecurity is generally treated as one element of a larger transformation agenda rather than as a cross-cutting governance condition linking institutional accountability with regulatory compliance, resilience and continuity.

A further contextual gap is found in the small body of research relating to Ukraine. Nashynets-Naumova et al. (2020) address information and cybersecurity technologies in the system of Ukrainian higher education institutions, and Kobis et al. (2024), in a comparative study of universities in Poland, Ukraine and the Czech Republic, highlight the significance of employees' views on information security and of training needs in the handling of digital resources. These papers confirm that technological protection and human capability matter in the Ukrainian case. They stop short, however, of offering a comprehensive account of the relationship between university-level practice, national cybersecurity governance arrangements, statutory obligations, institutional accountability, and the strategic dimension of higher education digitalisation.

Finally, institutional sustainability is itself related to cybersecurity. Othman (2023) connects hijackability as a factor in the survivability of higher education institutions with their ability to withstand cyberattacks, illustrating through a qualitative case study that institutions are under assault on multiple fronts and must enhance their cybersecurity governance. The single-case design, however, limits the transferability of these conclusions to other legal and institutional contexts.

The literature is thus scattered across three relatively insular areas: university-based cybersecurity management, national or ecosystem-level cyber governance, and higher education digital transformation. What has not yet emerged is a coherent analytical framework capturing the ways in which legal norms, public governance models, institutional duties, and university-level cybersecurity practices interrelate within a specific national higher education system. This divide is especially consequential for Ukraine, where digital transformation and cyber resilience must be built concurrently in a distinctive institutional and security context. The open research question is therefore not only what cybersecurity measures universities should take, but also how public governance can coordinate legal requirements, institutional capabilities, stakeholder obligations, and resilience mechanisms so that the digital transformation of higher education in Ukraine is both sustainable and secure.

3. Materials and Methods

The research was carried out in August–September 2026 as a qualitative policy analysis of legal and institutional documents governing cybersecurity in the context of Ukrainian higher education. The unit of analysis was the individual legal rule, policy instrument, institutionally mandated responsibility, or governance mechanism applicable to cybersecurity, cyber resilience, or the digital transformation of higher education institutions. The study involved no human subjects, surveys, experiments, interventions, or personal information.

The documentary evidence was treated not as a systematic-review sample but as an intentionally assembled analytical corpus. Non-random purposive sampling yielded 30 documents in two evidence groups: 19 peer-reviewed scientific publications and 11 official legal, strategic, and institutional documents. The scientific literature reviewed, produced mainly between 2019 and 2026, related to cybersecurity governance, information-security management in higher education, cyber resilience, institutional sustainability, and digital transformation. A publication was retained only where it supplied conceptual or governance resources directly applicable to the research problem.

The official-document group comprised four Ukrainian laws relating to higher education, cybersecurity, information protection, and critical infrastructure; the Cybersecurity Strategy of Ukraine; three EU legal instruments, namely the General Data Protection Regulation, the Cybersecurity Act and the NIS2 Directive; the Digital Education Action Plan 2021–2027; and two ENISA documents concerning cybersecurity competences and the current threat landscape. Only authoritative official or consolidated versions were used.

Sources were included if they were relevant to at least one of five substantive areas: cybersecurity in higher education institutions; national or institutional cybersecurity governance; legally defined cybersecurity responsibilities for public or educational organisations; the interplay between digital transformation, institutional resilience and higher education; or the legal status, governance responsibilities, institutional autonomy and organisational role of higher education institutions required to contextualise cybersecurity obligations. Duplicate publications, non-peer-reviewed opinion pieces, commercial web content, documents without clear analytical relevance, and studies confined to the technical aspects of attack detection without organisational or governance implications were excluded.

The analysis was conducted in four phases. First, the corpus was filtered through five a priori governance dimensions: legal mandate, distribution of institutional responsibility, inter-organisational coordination, university-level cybersecurity provision, and the embedding of cybersecurity in sustainable digital transformation. Sustainable digital transformation was understood as continuity, cyber resilience, secure digital infrastructure, institutional capacity, and the minimisation of deterioration in digital function under conditions of cyber risk. Second, the relevant provisions and findings were entered into a structured coding matrix recording source, level of governance, responsible actor, regulatory or organisational modality, compliance and enforcement requirements, and identified governance gap. The degree of HEI-specific regulatory specification was further categorised as direct, partial, indirect or absent, according to whether a source directly regulated higher education, addressed HEIs as a subgroup of more general regulated entities, offered only generic

rules or guiding principles applicable to HEIs, or contained no discernible sector-relevant rule. Third, the national policy framework was analysed for coherence between national strategic priorities, the sectoral legal framework, and the duties entrusted to higher education institutions. Fourth, these arrangements were compared with a selection of EU and ENISA instruments in order to identify convergence, partial harmonisation, institutional fragmentation, and residual governance challenges.

This final interpretative step linked formal legal requirements with documented institutional arrangements and aggregated recurrent relationships into a five-level governance structure comprising national, sectoral, institutional, operational, and assurance functions. Particular attention was paid to the explicit allocation of responsibility, to coordination mechanisms, to the role of universities as regulated organisations or governance actors, and to the incorporation of cybersecurity into digital-transformation policy. Because the design rests only on documentary evidence, the paper evaluates the formal governance architecture and documented institutional arrangements, not the actual performance of cybersecurity practice in individual Ukrainian universities.

4. Results

4.1. Legal mandate and the position of higher education institutions within the cybersecurity framework

The documentary coding reveals a structural asymmetry in the governance relationship. Although Ukraine has a broad general legal regime for cybersecurity and information protection, higher education does not appear within that regime as a distinct area of cybersecurity governance. The Law of Ukraine on the Basic Principles of Cybersecurity defines the national cybersecurity system and its principal public actors, establishes the mechanism for coordination, and imposes certain cybersecurity obligations on ministries and other public authorities, operators of critical infrastructure, owners or administrators of critical information infrastructure, and a number of other entities whose activities relate to national information resources, e-services, communications, information protection or cyber protection (Verkhovna Rada of Ukraine, 2017). The Cybersecurity Strategy places particular emphasis on cyber resilience, cooperation, national capacity building and the interaction of cybersecurity actors as conditions of Ukraine's existence in the digital domain (President of Ukraine, 2021).

This national mandate bears only indirectly on higher education, since no specific sectoral regime exists. Under the Law of Ukraine on Higher Education, a higher education institution is a separate legal entity possessing institutional autonomy in educational, research, organisational, economic, and personnel matters (Verkhovna Rada of Ukraine, 2014). Universities therefore have the organisational freedom to formulate internal cybersecurity policies, roles, and responsibilities, to manage their infrastructure and to allocate resources. The coding did not, however, identify in the higher education legislation analysed any sector-wide cybersecurity governance framework that would impose a common set of cyber-resilience functions on university governing bodies, define cybersecurity leadership roles, or create a standardised higher education incident-governance mechanism.

The Law of Ukraine on Protection of Information in Information and Communication Systems operates at a different regulatory level. It provides the legal framework for protecting information processed in information and communication systems, and therefore imposes obligations wherever university systems process information protected by statutory requirements (Verkhovna Rada of Ukraine, 1994). The Law of Ukraine on Critical Infrastructure introduces a resilience-focused regime covering continuity, recoverability, integrity, and the protection of critical infrastructure; its requirements become institutionally determinative for a university only where the relevant infrastructure is identified and treated under the critical-infrastructure regime, and not simply because the organisation is a higher education institution (Verkhovna Rada of Ukraine, 2021).

The results of coding these instruments against the five predefined dimensions are summarised in Table 1.

Table 1. Legal and institutional coverage of cybersecurity governance dimensions in Ukrainian higher education

Governance dimension	Documentary finding in the Ukrainian framework	Degree of HEI-specific specification	Identified governance gap
Legal mandate	Cybersecurity, information protection, cyber resilience, and critical-infrastructure protection are regulated at national level	Partial	No dedicated cybersecurity governance regime for the higher education sector
Institutional responsibility	National cybersecurity actors and broad categories of responsible entities are legally identified	Partial	University governing bodies and cybersecurity leadership functions are not standardised sector-wide
Inter-organisational coordination	National coordination and incident-response architecture exists	Partial	No uniform HEI-specific coordination channel linking universities, education authorities, and national cyber actors was identified
University-level arrangements	HEIs possess organisational autonomy and may establish internal structures and policies	Indirect	Autonomy does not itself define minimum governance roles, reporting chains, or cyber-resilience functions
Cybersecurity and digital transformation	National strategy connects cybersecurity with secure digital development	Partial	Higher education digitalisation and cybersecurity governance remain institutionally separated across the analysed legal instruments

Note. HEI = higher education institution. „Partial" means that the relevant governance element is present in the broader legal framework but is not comprehensively specified for higher education as a sector. Source. Compiled by the author on the basis of Verkhovna Rada of Ukraine (1994, 2014, 2017, 2021) and President of Ukraine (2021).

The table shows that the central weakness is not the absence of cybersecurity legislation. Instead, the relevant mechanism is the explicit sectoral translation of national cybersecurity requirements to the autonomous governance structures of universities. The distinction matters, because the scientific literature consistently describes higher education as a hetero-

geneous environment of users, distributed information systems, open academic networks, research data, and varied institutional assets (Nashynets-Naumova et al., 2020; Merchan-Lima et al., 2021; Afolalu & Tsoeu, 2025). General organisational obligations therefore do not necessarily define how responsibility is allocated within a university.

4.2. Allocation of responsibility and inter-organisational coordination

The second dimension of the coding concerned the distribution of duties. Here the Ukrainian model proved relatively well developed at national level and less well defined at university level. The Law on the Basic Principles of Cybersecurity establishes a multi-actor framework that includes, within their respective areas of competence, the State Service of Special Communication and Information Protection, the National Police, the Security Service of Ukraine, defence and intelligence bodies, the National Bank, and the Ministry of Foreign Affairs, among others. It also provides for information sharing, incident response, preventive measures, training, cybersecurity audit, and public–private collaboration within the national system (Verkhovna Rada of Ukraine, 2017). The Cybersecurity Strategy echoes this network logic, conceptualising cyber resilience as the product of interaction among cybersecurity actors rather than of protection at the level of a single organisation (President of Ukraine, 2021).

At the level of the individual HEI, however, the documentary corpus does not disclose a comparable predefined chain of responsibility running from the rectorate or governing body to an accountable cybersecurity executive, an operational cybersecurity team, data and system owners, and users. The university autonomy provided for in the higher education law permits such arrangements but does not require them as a matter of cybersecurity governance (Verkhovna Rada of Ukraine, 2014). This produces a governance arrangement in which national accountability is relatively well specified while organisational translation continues to depend on institutional decisions.

The scientific evidence makes this gap all the more salient in practice. Reviews of information security management in higher education describe competence, resources, guidance, security frameworks, and implementation strategy as dynamically related rather than as isolated elements (Merchan-Lima et al., 2021). Recent reviews also show that fragmented security arrangements, low levels of awareness, insufficient training, poor incident reporting, and technical gaps are found even among digitally mature organisations (Afolalu & Tsoeu, 2025; Salam et al., 2026). Findings relating to universities in Ukraine likewise suggest that the way employees act and are trained in security remains a factor in protecting the institution's digital assets (Kobis et al., 2024). The evidence thus suggests that cyber resilience entails not simply a legal obligation to protect systems but also a specified organisational route through which that obligation is to be discharged.

The distinction is laid bare more clearly by the European comparison. Under the GDPR, liability lies with the controller, and technical and organisational measures must be proportional to the risk of processing; security is defined as including confidentiality, integrity, availability, resilience, the capacity for restoration and the periodic evaluation of measures (European Parliament & Council of the European Union, 2016). The relevance of this model

to the present comparison is not that the GDPR supplies a comprehensive cybersecurity framework for universities, but that it ties legal accountability to demonstrable organisational action.

NIS2 strengthens this governance logic further. It imposes on entities within its scope a duty to take appropriate and proportionate cybersecurity risk-management measures, and it locates accountability at management level. Member States may provide for the Directive to apply to education institutions, in particular those carrying out critical research activities (European Parliament & Council of the European Union, 2022); that possibility does not make every university an NIS2 entity. What it does show is a regulatory route by which higher education can be brought expressly within a national framework of cyber-risk governance, rather than addressed only in general terms.

4.3. University-level cybersecurity arrangements

The third dimension concerned the governance required within the university itself. Four functional requirements recurred across the scientific and institutional corpus: strategic cybersecurity leadership, risk and compliance management, incident response, and continuous competence development. The Ukrainian legal framework supports these functions but does not combine them into a standard HEI governance model.

The ENISA European Cybersecurity Skills Framework provides a useful organisational benchmark, because it converts cybersecurity from an abstract institutional obligation into professional functions that can be identified. Its twelve cybersecurity role profiles cover cybersecurity leadership, risk, incident response, architecture, implementation, auditing, threat intelligence, and other areas (European Union Agency for Cybersecurity, 2022). The CISO-level profile in particular links organisational cybersecurity with strategy, policy, senior-management involvement, information security management systems, reporting, external collaboration, resource allocation, resilience, and capacity building. For universities, this makes visible the governance difference between employing IT staff and establishing accountable cybersecurity functions.

The Cybersecurity Act adds a second dimension to this institutional benchmark. It does not seek to mandate the governance structure of universities, but defines the role of ENISA and establishes a European cybersecurity certification framework for ICT products, services and processes, with risk-based assurance levels and a common certification approach (European Parliament & Council of the European Union, 2019). For HEIs increasingly reliant on cloud services, digital learning platforms, identity services, research infrastructure, and externally provided ICT products, this adds a supply-side governance dimension absent from a narrow perimeter-protection model.

The current threat landscape further supports this wider institutional view. Phishing was the leading intrusion vector in the EU threat landscape analysed in ENISA's 2025 threat assessment, ransomware continued to be one of the most high-impact threats, and increasing reliance on digital dependencies amplified risk across interconnected digital ecosystems (European Union Agency for Cybersecurity, 2025). These findings align with evidence at HEI level showing continuing vulnerability to phishing, malware, weak credentials, software

vulnerabilities, intellectual property risk, low levels of awareness and poor incident practice (Afolalu & Tsoeu, 2025; Salam et al., 2026). The overall conclusion is that university cybersecurity governance must address people, organisational responsibility, systems, external providers, and response capacity. No single technical department, lacking institution-wide authority, can govern all five areas on its own.

4.4. Cybersecurity as a condition of sustainable digital transformation

The fourth and fifth coding dimensions converged on the relationship between cybersecurity and digital transformation. The Digital Education Action Plan treats successful digital transformation as dependent on infrastructure, institutional strategy, leadership, organisational capability, skills, safe environments, privacy, and cooperation among education providers, institutions, technology companies, and other relevant parties (European Commission, 2020). This contrasts with a model in which security is layered on once digital systems have been chosen and implemented.

The documentary comparison accordingly revealed a sequencing problem for Ukrainian HEIs. Decentralised digital innovation is underpinned by higher education autonomy, while cybersecurity legislation establishes a national architecture of protection duties and response. The documents analysed do not, however, merge these two governance routes into a single sector-specific cycle in which digitalisation decisions give rise to cybersecurity risk management, institutional liability, skills development, incident preparedness, supplier management, and a review-based management of these activities.

This distinction is summarised by comparing the Ukrainian architecture with selected EU and ENISA instruments. Table 2 reports the comparative outcome rather than legal equivalence between the two systems.

Table 2. Comparative governance assessment of Ukrainian HEIs against selected EU and ENISA benchmarks

Governance element	Ukrainian documentary position	Selected EU/ENISA benchmark	Comparative result
Management accountability	Broad organisational and statutory responsibility; no uniform HEI cybersecurity leadership model identified	GDPR accountability; NIS2 management-level responsibility for covered entities	Partial alignment
Risk-based security	Present through information protection, cybersecurity, and critical-infrastructure regimes	Explicit risk-based technical and organisational measures in GDPR and NIS2	Substantive basis exists, but HEI operationalisation is fragmented
Incident governance	National incident-response and coordination mechanisms exist	NIS2 formalises organisational risk management and incident reporting for entities within scope	National capacity stronger than HEI-specific procedural specification
Professional cybersecurity roles	Not standardised across HEIs by higher education legislation	ECSF defines interoperable cybersecurity role profiles and competences	Clear institutionalisation gap

Governance element	Ukrainian documentary position	Selected EU/ENISA benchmark	Comparative result
Secure digitalisation	Cybersecurity and higher education digitalisation are governed through separate legal and policy streams	Digital Education Action Plan integrates strategy, leadership, secure platforms, privacy, skills, and collaboration	Partial policy convergence, weak sectoral integration
ICT assurance and supply chain	General protection obligations apply; HEI-specific procurement assurance not identified in the analysed corpus	Cybersecurity Act provides EU-level certification architecture for ICT products, services, and processes	Comparative gap in explicit HEI-oriented assurance mechanisms
Higher education sector coverage	HEIs enter cybersecurity regulation primarily through general or conditional legal categories	NIS2 allows Member States to extend scope to education institutions, especially those conducting critical research	Sectoral coverage remains less explicit in Ukraine

Note. The EU instruments are used as comparative regulatory and policy benchmarks, not as evidence that every provision applies directly to every Ukrainian HEI. NIS2 coverage of educational institutions depends on the scope established by Member States and on other conditions of the Directive. Source. Compiled by the author on the basis of European Commission (2020), European Parliament and Council of the European Union (2016, 2019, 2022), European Union Agency for Cybersecurity (2022), Verkhovna Rada of Ukraine (1994, 2014, 2017, 2021), and President of Ukraine (2021).

4.5. Integrated governance finding

The final stage of interpretation produced a five-tier governance structure arising from the relationships identified rather than from any single determinant. At the first level, national cybersecurity policy defines strategic goals, baseline requirements, coordination, and response capability. At the second, sectoral governance should convert those general aims into requirements suited to the higher education context, including through differentiated treatment of institutions whose research, information resources, or infrastructure carry elevated risk. At the third, university governing bodies need to assign responsibility, approve cybersecurity policy and risk tolerance, endorse resource requirements, and embed cyber resilience in the institution's digital strategy. At the fourth tier, operational roles include information-security management, incident response, access and identity management, data protection, infrastructure and supplier risk, awareness, and continuity. The fifth tier is a continuous assurance loop drawing on incident data, risk reassessment, audits or evaluations, capability development, and the revision of organisational policy.

The coding matrix suggests that the components of this structure do exist in Ukraine, but in different legal and institutional layers. National coordination and cybersecurity policy are relatively clear; the protection of information systems is mandated by law; critical-infrastructure legislation imposes resilience-based obligations where applicable; and higher education law grants significant organisational freedom (Verkhovna Rada of Ukraine, 1994, 2014, 2017, 2021). It is the intermediate layer connecting the national system to the internal administration of an ordinary HEI that remains loosely institutionalised.

The main finding emerging from the doctrinal comparison is therefore one of institutional fragmentation rather than of regulatory absence. Ukrainian universities operate at the intersection of higher education autonomy, the demands of national cybersecurity gover-

nance, critical-infrastructure regulation where applicable, and expanding digital infrastructure provisions. The framework analysed does not, however, bring these elements together into a unified sectoral governance model that would specify at least minimum university-level cybersecurity duties, management accountability, professional functions, coordination channels, cyber-resilience planning, and integration with institutional digital-transformation strategies.

The EU comparison suggests that these gaps in connection need not be accepted as the price of university autonomy. The European instruments selected show, on the contrary, how decentralised organisational responsibility can be combined with risk-based accountability, management oversight, competence frameworks, secure digital platforms, certification schemes, and inter-institutional coordination (European Commission, 2020; European Parliament & Council of the European Union, 2016, 2019, 2022; European Union Agency for Cybersecurity, 2022). In the Ukrainian context, the governance arrangement to be built from these models is therefore not a parallel cybersecurity bureaucracy for the higher education sub-sector, but the formal linkage of the self-governing university to the wider national cybersecurity architecture through sector-specific minimum duties, interface specifications, and cyber-resilience standards.

5. Discussion

The main contribution of this paper is to show that the governance of cybersecurity in Ukrainian higher education is not so much unregulated between national higher education and cybersecurity policy as it is differentiated across levels — national policy, subsystems of higher education governance, and university-level institutional arrangements. Ukraine now possesses legal instruments for the protection of information, the coordination of cybersecurity, the resilience of critical infrastructure, and institutional autonomy. What remains missing or underdeveloped is the intermediate, or „meso", level of governance that translates these national requirements into a consistent and intelligible set of responsibilities for higher education institutions. That distinction is crucial, because it moves the policy challenge away from creating further cybersecurity rules and towards integrating the regulatory and organisational components that already exist.

This conclusion accords in general terms with research from other countries suggesting that weak cybersecurity on university campuses is not attributable solely to deficits in technical protection. Fragmented information security management and weak institutional cooperation were identified as problems facing higher education by Bongiovanni (2019). Merchan-Lima et al. (2021) proceed along the same lines, showing that universities adopt diverse security models and approaches to infrastructure and network management, as do Imbaquingo-Esparza et al. (2022), who find that growing reliance on digital technology increases organisation-level information security risk. The findings presented here develop these insights further by identifying fragmentation not only within the organisation of security in universities but also between that organisation and the broader public-governance framework.

This deficient division of labour in responsibilities is also consistent with the emphasis

on governance rather than control advanced by Kuerbis and Badiei (2017) and Savaş and Karataş (2022). Their work conceptualises cybersecurity as an emergent effect of interaction between hierarchical, networked and organisational structures, and therefore as a responsibility that cannot be located in a single public authority. The present results suggest that this is particularly true of Ukrainian higher education. National cyber bodies can offer strategic direction and incident-response capacity, but university autonomy means that operational responsibility remains decentralised. Autonomy is thus not incompatible with stronger cybersecurity governance; on the contrary, it increases the need for clear interfaces between public and institutional decision-making.

The contrast with Carmichael's (2026) study of Estonia further substantiates this reading. Estonia provides representative evidence that even the most „mature" digital states continue to renegotiate the distribution of cybersecurity responsibilities across institutions. Although Ukraine differs radically in institutional history and securitisation context, the comparison implies that mature cyber governance depends on continually clarifying the configuration of responsibilities rather than on fixing it. For Ukrainian HEIs, the open question is therefore not what responsibility to centralise, but which responsibilities are best institutionalised at university level and which are best addressed sectorally.

Two of the paper's principal findings concern the relationship between cybersecurity and digital transformation. The Ukrainian framework analysed here addresses the two spheres through somewhat divergent policy strands. This separation runs contrary to the change literature, which conceptualises organisational strategy, leadership, digital solutions, resources, organisational infrastructure and institutional culture as convergent constructs. Castro Benavides et al. (2020) argue that digital transformation in higher education demands an institution-level approach, and Fernández et al. (2023) hold that transformation succeeds when it is approached from the technological, organisational, process and human levels. Farias-Gaytan et al. (2023) support this line by connecting digital transformation with institutional capacities and digital literacy. The present findings indicate that cybersecurity might better be viewed as a further cross-cutting aspect of this transformation than as a technical exercise carried out after digital systems have been deployed.

This understanding is confirmed, significantly, by studies of barriers to digital transformation. Gkrimpizi et al. (2023) differentiate barriers that are strategic, organisational, technological, cultural and human, and Singun (2025) highlights the relevance of leadership, resources, competences, stakeholder management, and institutional culture. The governance gaps identified in this study are precisely of that kind. A university may possess technically adequate security tools and yet remain institutionally vulnerable if its policies on accountability, competence, supplier governance, incident escalation and continuity are unclear.

The Ukrainian evidence also partially corresponds with Nashynets-Naumova et al. (2020), who identify technological and organisational solutions to information and cybersecurity problems in Ukrainian HEIs, and with Kobis et al. (2024), whose comparative evidence underlines the importance of employee practice and security training. The present analysis nevertheless shows that competence building is not sufficient on its own. The organisational benefit of training depends on whether cybersecurity roles and chains of responsibility are institutionally defined. This finding is consistent with Nuñez et al. (2023), who show the

necessity of integrating technical tools, organisational controls, standards, and institutional practice.

Finally, the relationship between cybersecurity governance and institutional resilience is consistent with Othman (2023), for whom the risk of cyberattack has consequences for the long-term viability of higher education institutions. The present study extends that conclusion: sustainability depends not only on an institution's capacity to respond to individual incidents, but also on embedding cyber resilience in the governance of digital transformation. The continued prevalence of phishing, malware, credential compromise, vulnerabilities, and human-factor risk in HEIs is documented by Afolalu and Tsoeu (2025) and Salam et al. (2026). The present findings help explain why these threats call for governance responses covering management accountability, professional competence, coordination, suppliers, continuity, and institutional learning.

The study is limited by its documentary character. It identifies formal responsibilities and governance structures but cannot determine how reliably they are carried out in individual Ukrainian universities. Future research should therefore investigate the institutional cybersecurity policies, organisational structures, incident-response procedures, staffing models, and governance practices of a range of Ukrainian HEIs. The present findings nevertheless provide a foundation for that inquiry: improving cybersecurity in Ukrainian higher education does not require a parallel regulatory framework, but a sector-specific governance layer that bridges the gap between the national cybersecurity architecture and autonomous university management, alongside sustainable digital transformation.

6. Conclusions

The research has shown that the governance of cybersecurity in Ukrainian higher education rests on a robust national legal and strategic framework, but that this framework is not yet sufficiently elaborated in a sector-specific model for HEIs. Analysis of the 30-document corpus revealed that legal obligations concerning cybersecurity, information protection, critical infrastructure, organisational autonomy, and digital maturity are dispersed across different layers of regulation and institution. The principal weakness is therefore not regulatory absence but the weak coordination between national-level cybersecurity governance and university-level responsibility.

Five aspects of governance were examined: legal mandate, institutional responsibility, inter-organisational coordination, university-level cybersecurity provision, and the integration of cybersecurity into sustainable digital transformation. The analysis indicated that, although national-level guidance is comparatively strong, there is only partial definition of what cybersecurity leadership, accountability structures, incident involvement, professional functions, and sector-wide resilience requirements should look like for higher education.

An implication for practice is that Ukraine does not need a separate parallel cybersecurity system for universities. A more adequate way forward would be to create a sectoral governance layer connecting autonomous university governance with the national cybersecurity architecture. This should include a minimum institutional duty of care, management accountability, coordination mechanisms, competence requirements, cyber-resilience plan-

ning, and the embedding of cybersecurity within digital-transformation strategies.

As documentary research, this study cannot trace how formal requirements are executed, how policies influence practice in particular universities, or how effective institutionalised practices prove in operation. Comparative studies of cybersecurity governance across different types of Ukrainian HEI should be developed to examine their internal policies, incident-response capabilities, staffing, competence, supplier-risk management, and continuity mechanisms. Empirical substantiation would move the governance logic proposed here towards a practical sectoral model for sustainable and secure digital transformation.

Two implications follow for regulatory practice, and they are the reason the analysis belongs to the study of law, digital technologies and sustainable governance rather than to information security alone. First, the instrument that will determine whether a Ukrainian university actually governs its cyber risk is not the national statute but the subordinate sectoral rule that has not yet been made. For as long as the connection between the national cybersecurity architecture and autonomous institutional governance is left to each university to devise for itself, the standard achieved will track institutional capacity rather than legal obligation. Regulators and education authorities should therefore attend to the design of that intermediate layer, and not only to the adequacy of the primary legislation. Second, sectoral coordination of this kind is a condition of sustainability and not only of security: where digitalisation decisions are taken without a defined route to responsibility, competence and continuity, the digital capacity that results is not durable. On this reading, the task facing Ukrainian higher education is less the enactment of new cybersecurity norms than the institutional translation of the norms that already exist.

Funding Statement

This research received no external funding.

Conflicts of Interest

The author declares no conflicts of interest.

Ethical Approval Statement

This study was conducted as a documentary analysis of publicly available legal, strategic, policy and scholarly sources. There were no human subjects, surveys, experiments, interventions, or personal information. Formal ethics committee approval was therefore not required.

References

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. Future Internet, 17(12), Article 575. https://doi.org/10.3390/fi17120575

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on informa-

tion security management in higher education. Computers & Security, 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Boutemeur, J., Lella, I., Bakatsis, I., Chatzichristos, G., Foley, K., Leskinen, J., Otcenasek, J., & Ziolek, D. (2025). ENISA threat landscape 2025. European Union Agency for Cybersecurity. https://doi.org/10.2824/1946374

Carmichael, L. (2026). Crafting a cybersecurity governance ecosystem: Two decades of learning in Estonia. European Policy Analysis, 12(2), Article e70017. https://doi.org/10.1002/epa2.70017

Castro Benavides, L. M., Tamayo Arias, J. A., Arango Serna, M. D., Branch Bedoya, J. W., & Burgos, D. (2020). Digital transformation in higher education institutions: A systematic literature review. Sensors, 20(11), Article 3291. https://doi.org/10.3390/s20113291

Chornomydz, A. V. (2025). Faculty information security in higher education institutions amidst martial law: Challenges and practical guidelines. Medical Education, (2), 67–71. https://doi.org/10.11603/m.2414-5998.2025.2.15490

Cotta, B., & Righettini, M. S. (2026). Governing cybersecurity in the digital age: Mapping comprehensive policy mixes with the Nodality-Authority-Treasure-Organization lens. Review of Policy Research, 43(4), Article e70113. https://doi.org/10.1111/ropr.70113

European Commission. (2020). Digital Education Action Plan 2021–2027: Resetting education and training for the digital age (COM(2020) 624 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament & Council of the European Union. (2019). Regulation (EU) 2019/881 of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj

European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union Agency for Cybersecurity. (2022). European Cybersecurity Skills Framework (ECSF). https://doi.org/10.2824/859537

Farias-Gaytan, S., Aguaded, I., & Ramirez-Montoya, M.-S. (2023). Digital transformation and digital literacy in the context of complexity within higher education institutions: A systematic literature review. Humanities and Social Sciences Communications, 10, Article 386. https://doi.org/10.1057/s41599-023-01875-9

Fernández, A., Gómez, B., Binjaku, K., & Meçe, E. K. (2023). Digital transformation initiatives in higher education institutions: A multivocal literature review. Education and Information Technologies, 28(10), 12351–12382. https://doi.org/10.1007/s10639-022-11544-0

Gkrimpizi, T., Peristeras, V., & Magnisalis, I. (2023). Classification of barriers to digital transformation in higher education institutions: Systematic literature review. Education Sciences, 13(7), Article 746. https://doi.org/10.3390/educsci13070746

Imbaquingo-Esparza, D., Díaz, J., Ron Egas, M., Fuertes, W., & Molina, D. (2022). Information security at higher education institutions: A systematic literature review. In J. Herrera-Tapia, G. Rodriguez-Morales, E. R. Fonseca C., & S. Berrezueta-Guzman (Eds.), Information and communication technologies: 10th Ecuadorian Conference, TICEC 2022, Manta, Ecuador, October 12–14, 2022, proceedings (pp. 294–309). Springer.

https://doi.org/10.1007/978-3-031-18272-3_20
Kobis, P., Kisiołek, A., Karyy, O., Pawliczek, A., & Chmielarz, G. (2024). Selected aspects of information security in e-marketing activities of higher education institutions in Poland, Ukraine and the Czech Republic. Procedia Computer Science, 246, 4617–4626. https://doi.org/10.1016/j.procs.2024.09.326
Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. Digital Policy, Regulation and Governance, 19(6), 466–492. https://doi.org/10.1108/DPRG-05-2017-0024
Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: A systematic review. Annals of Telecommunications, 76(3–4), 255–270. https://doi.org/10.1007/s12243-020-00783-2
Nashynets-Naumova, A. Y., Buriachok, V. L., Korshun, N. V., Zhyltsov, O. B., Skladannyi, P. M., & Kuzmenko, L. V. (2020). Technology for information and cyber security in higher education institutions of Ukraine. Information Technologies and Learning Tools, 77(3), 337–354. https://doi.org/10.33407/itlt.v77i3.3424
Nuñez, M., Palmer, X.-L., Potter, L., Aliac, C. J., & Velasco, L. C. (2023). ICT security tools and techniques among higher education institutions: A critical review. International Journal of Emerging Technologies in Learning, 18(15), 4–22. https://doi.org/10.3991/ijet.v18i15.40673
Othman, Z. (2023). Sustainability of higher education institutions: Case study on cyber attacks. Global Business Management Review, 15(1), 24–38. https://doi.org/10.32890/gbmr2023.15.1.2
President of Ukraine. (2021, August 26). Decree No. 447/2021 on the decision of the National Security and Defense Council of Ukraine of 14 May 2021 „On the Cybersecurity Strategy of Ukraine". https://zakon.rada.gov.ua/laws/show/447/2021
Salam, M., Abu Bakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2026). Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities. SAGE Open, 16(1). https://doi.org/10.1177/21582440251413473
Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7–34. https://doi.org/10.1365/s43439-021-00045-4
Singun, A. (2025). Unveiling the barriers to digital transformation in higher education institutions: A systematic literature review. Discover Education, 4, Article 37. https://doi.org/10.1007/s44217-025-00430-9
Verkhovna Rada of Ukraine. (1994, July 5). Law of Ukraine No. 80/94-VR on protection of information in information and communication systems [as amended]. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
Verkhovna Rada of Ukraine. (2014, July 1). Law of Ukraine No. 1556-VII on higher education [as amended]. https://zakon.rada.gov.ua/laws/show/1556-18
Verkhovna Rada of Ukraine. (2017, October 5). Law of Ukraine No. 2163-VIII on the basic principles of cybersecurity in Ukraine [as amended]. https://zakon.rada.gov.ua/laws/show/2163-19
Verkhovna Rada of Ukraine. (2021, November 16). Law of Ukraine No. 1882-IX on critical infrastructure [as amended]. https://zakon.rada.gov.ua/laws/show/1882-20