

18. United Nations. E-Government Survey 2024. URL: <https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2024>
19. Hacker P. Regulating ChatGPT and Other Large Generative AI Models. In: FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. 2023. P. 1112–1123. URL: <https://doi.org/10.1145/3593013.3594067>
20. European Commission. European Declaration on Digital Rights and Principles for the Digital Decade. 2023. URL: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023C0123\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023C0123(01))
21. European Commission. The Digital Decade Policy Programme 2030. URL: <https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030>
22. European Commission. Shaping Europe's Digital Future. URL: <https://digital-strategy.ec.europa.eu/en>
23. Novelli C., Hacker P., Morley J., Trondal J., Floridi L. A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. European Journal of Risk Regulation. 2024. P. 1–25. URL: <https://doi.org/10.1017/err.2024.57>

1.3. Institutional and regulatory frameworks for information security in the context of digital transformation: the experience of European Union countries and the adaptation of Ukrainian legislation

*Svitlana ONYSHCHENKO,
Oleksandra MASLIY
National University “Yuri Kondratyuk
Poltava Polytechnic”*

The digital transformation of the economy and society is fundamentally altering not only the technological environment but also the very approach to state regulation, risk management and the assurance of information security. The development of artificial intelligence, digital platforms and network infrastructure requires the

simultaneous establishment of an appropriate institutional and legal framework capable of ensuring the security, resilience and accountability of digital processes. Otherwise, a regulatory gap and a mismatch arise between the pace of technological change and the capacity of the state and society to develop the legal, organisational and technical mechanisms required to manage new risks promptly.

Over the past decade, the European Union has developed one of the world's most comprehensive information security regulatory frameworks, encompassing personal data protection, the cybersecurity of critical infrastructure, the security of digital products and the liability of digital platforms. Meanwhile, it is important to clearly distinguish between two levels of analysis of this system, which are often confused in academic discourse despite being essentially different in scope for scholarly research. The first level is supranational, represented by EU directives and regulations establishing minimum harmonised standards for all Member States. The second level is the national level, where each Member State implements these standards through the lens of its own institutional traditions, administrative culture, and security context; as a result, the practical architecture of information security varies significantly even within the EU's single legal space. The divergence of these national models, despite the formal unity of the underlying regulatory framework, is precisely what makes a comparative analysis necessary; without it, the harmonisation of Ukrainian legislation with the EU acquis risks being reduced to a mere formal copying of the texts of directives, without taking into account the institutional prerequisites that make these provisions effective in practice.

This distinction matters for Ukraine not merely in theory but also in practice. The experience of previous rounds of EU expansion, particularly the 2004 Central European wave, represented by Estonia and Poland, demonstrates that the formal adoption of transposed legislation (known as 'paper harmonisation') is a necessary but obviously inadequate condition for functional compliance with the EU acquis. Genuine compliance requires the development of institutional capacity – namely, in terms of human resources, finance and organisation – capable of applying the adopted rules in practice.

The EU's regulatory framework for information security was established not as a single act, but as a series of interlinked legal instruments, each of which addressed the new challenges posed by the next stage of digital transformation.

The cornerstone of the entire personal data protection framework remains [Regulation \(EU\) 2016/679 of the European Parliament and of the Council 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 \(General Data Protection Regulation, GDPR\)](#), which became applicable on 25 May 2018. The GDPR introduced a harmonised approach to the processing of personal data across the European Union, enshrining the principles of lawfulness, transparency, purpose limitation and data minimisation. It also established substantial administrative fines of up to EUR 20 million or 4% of the total worldwide annual turnover and, importantly, extended the territorial scope of its provisions to certain controllers and processors established outside the Union where they process the personal data of data subjects in the Union in connection with the offering of goods or services or the monitoring of their behaviour. The Regulation has effectively become an influential global regulatory benchmark, commonly associated in academic literature with the “Brussels effect”, subsequently shaping data protection legislation and regulatory practices in numerous jurisdictions beyond the European Union.

The first horizontal cybersecurity instrument was Directive (EU) 2016/1148 (NIS Directive), which established the initial requirements for operators of essential services and digital service providers. Its practical implementation revealed significant shortcomings, including fragmented approaches across the Member States, a limited range of regulated sectors, and weak mechanisms for cross-border coordination. In response, [Directive \(EU\) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union \(NIS2 Directive\)](#) was adopted (European Parliament and Council of the European Union, 2022). It entered into force on 16 January 2023.

NIS2 has significantly expanded the scope of regulation by introducing a distinction between “essential entities” and “important entities”, depending on the type, size and significance of their activities. The scope of the Directive covers 18 sectors,

grouped into two categories: 11 high-criticality sectors and 7 other critical sectors. These include energy, transport, the banking sector, financial market infrastructure, healthcare, water supply and sanitation, digital infrastructure, ICT service management, public administration, the space sector, postal and courier services, waste management, the production, manufacture and distribution of chemicals, the production, processing and distribution of foodstuffs, digital service providers and research organisations.

Another important regulatory development was the measures for managing cybersecurity risks set out in Article 21, which cover, in particular, policies on risk analysis and the security of information systems, incident response, business continuity and crisis management, supply chain security, cryptography and encryption, access control and multi-factor authentication. Article 23 establishes a multi-stage mechanism for the mandatory reporting of significant incidents: an early warning must be submitted within 24 hours of the entity becoming aware of the incident; a report on the incident must be submitted within 72 hours; and a final report must be submitted no later than one month after receipt of such a report.

Furthermore, the governing bodies of major and significant entities are required to approve measures for managing cybersecurity risks, monitor their implementation, and may be held liable for violating the relevant requirements; members of governing bodies must also undergo cybersecurity training. For breaches of the requirements of Articles 21 and 23, the maximum administrative fines for key entities shall be at least €10 million or 2 per cent of the total annual turnover for the previous financial year, and for significant entities – at least €7 million or 1.4 per cent of the relevant turnover, whichever is higher. Member States were required to transpose the provisions of the Directive into national law by 17 October 2024; nevertheless, as discussed in more detail below based on the example of Poland, this process has been delayed in several Member States.

In 2024, the regulatory framework was further complemented by [Regulation \(EU\) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements \(Cyber Resilience Act, CRA, 2024\)](#). For the first time at the EU level, the CRA introduces mandatory cybersecurity requirements at the design and development stages of

hardware and software, thereby embedding the principle of security by design. It also requires manufacturers to report identified vulnerabilities and actively exploited vulnerabilities within 24 hours and provides for CE marking as evidence of conformity. The Regulation entered into force on 12 November 2024 but will apply from 11 December 2027, thus providing the market with an extended transitional period for adapting production processes.

[Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services \(Digital Services Act, DSA, 2022\)](#), which entered into force on 16 November 2022 and has applied since 17 February 2024, complements the legal framework for information security by establishing requirements concerning the moderation of illegal content, the transparency of recommender systems, and the mitigation of systemic risks on very large online platforms. This dimension is of particular importance in the context of hybrid information operations faced by Ukraine.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 deserves special attention on ENISA (the EU Agency for Cybersecurity) and on the certification of information and communication technology cybersecurity (Cybersecurity Act, 2019), which has been in force since 27 June 2019. This legislation fulfils two functions. Firstly, it transformed ENISA, which had been operating since 2004 based on temporary mandates that were periodically renewed, into a permanent agency with a strengthened budget and expanded powers, particularly regarding operational cooperation, capacity-building in Member States and support during large-scale cyber incidents. Secondly, it established the European Cybersecurity Certification Scheme, under which ENISA, on behalf of the European Commission, develops candidate certification schemes for specific categories of ICT products, services and processes; each scheme defines security requirements, assessment methods and one of three levels of assurance – basic, substantial or high. Certificates issued under such a scheme are recognised in all Member States, replacing fragmented national certification schemes (such as the French CSPN or individual schemes of the German BSI) for the categories covered. The first and, to date, the main scheme is the EUCC (Common Criteria-based scheme), formally adopted by Commission Implementing Regulation (EU) 2024/482 in January 2024 and intended for the

certification of ICT hardware and software products, in particular microchips and smart cards; The EUCS scheme for cloud services and the EU5G scheme for fifth-generation networks are also at the development stage; their finalisation is being hampered by political disputes over digital sovereignty requirements concerning cloud service providers outside the EU.

It is worth noting that, unlike the approach involving the adoption of a single “cybersecurity law”, the EU’s regulatory model is structured as an ecosystem of coordinated horizontal and sector-specific instruments covering, simultaneously, data (GDPR), networks and organisations (NIS2), products (CRA), certification (Cybersecurity Act) and platforms (DSA). This multi-layered architecture is a deliberate institutional choice: it makes it possible to avoid excessive standardisation where the specific nature of sectors requires a differentiated approach, whilst ensuring horizontal consistency in the underlying principles of risk management.

A distinct area of concern within the EU regulatory environment is the governance of the data economy. Although it does not formally fall within the scope of cybersecurity legislation in the narrow sense, it directly shapes the security and trust framework governing cross-border data flows. [Regulation \(EU\) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance \(Data Governance Act, DGA, 2022\)](#), which entered into force on 23 June 2022 and has applied since 24 September 2023, establishes conditions for the re-use of protected public sector data, a mechanism for the notification and supervision of data intermediation services based on the principle of intermediary neutrality, as well as a framework for the voluntary registration of “data altruism” entities. This institutional and regulatory framework for information security is further complemented by Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act), which governs rights of access to data generated by connected products, including Internet of Things devices, and strengthens safeguards against unlawful cross-border requests for access to such data by public authorities of third countries.

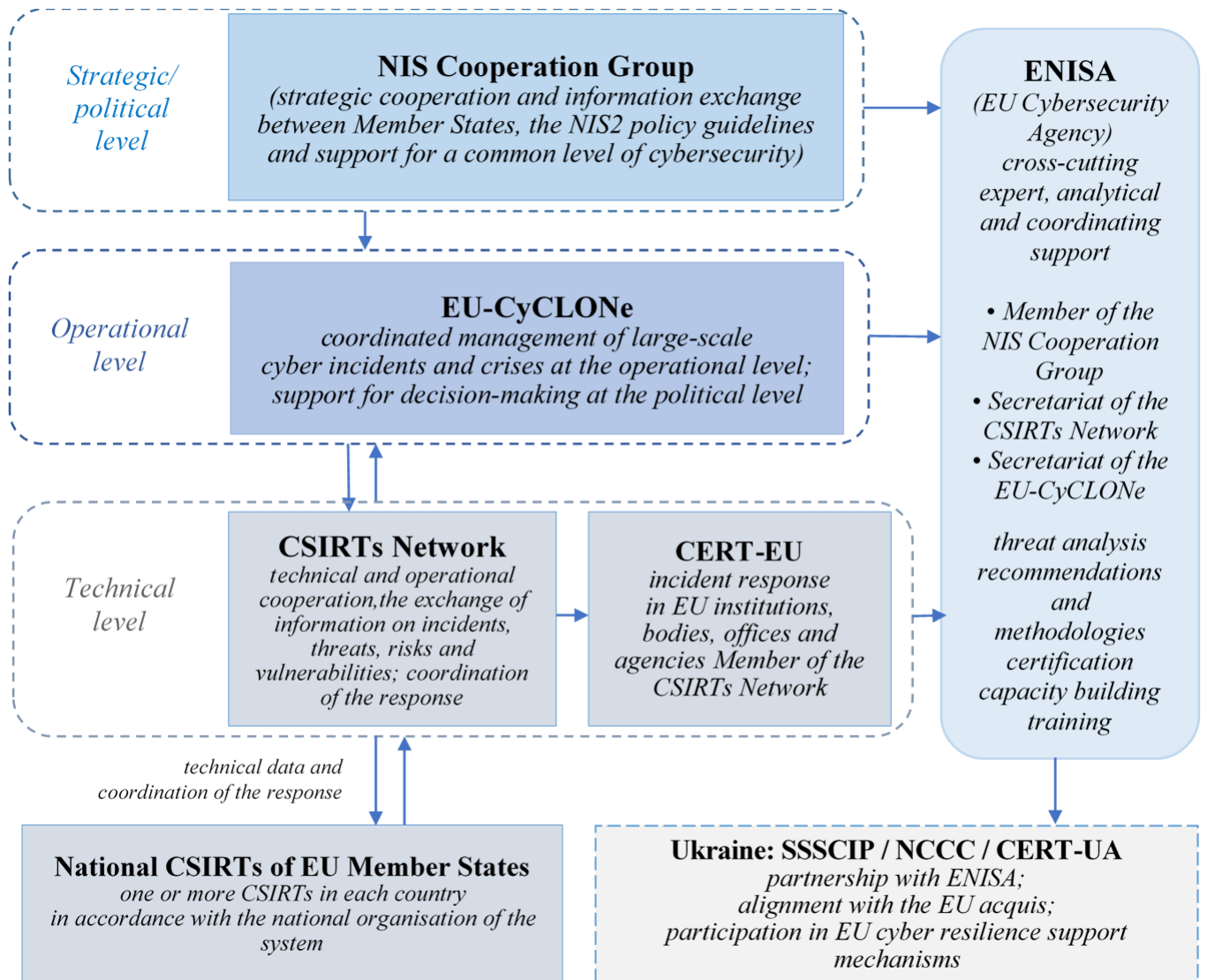
The significance of this regulatory approach for the issues facing the department is twofold. Firstly, it shapes the economic context within which the requirements of NIS2 and the GDPR are implemented: network security and the protection of personal data cannot be viewed in isolation from the broader infrastructure of trust for data

exchange that the DGA is building. Secondly, the logic underlying the DGA and the Data Act—which restricts cross-border access to data from third countries—is structurally akin to the French concept of digital sovereignty; both instruments are designed to safeguard critical data from jurisdictional influence outside the EU, which is directly relevant to the formulation of Ukrainian policy regarding the hosting of government data in the cloud infrastructures of foreign providers.

The effectiveness of the regulatory framework depends, first and foremost, on the level of institutional capacity for its practical implementation. In this regard, the European Union has established a multi-level coordination system, structured across three hierarchical levels. This model (strategic/political, operational and technical levels) serves as an example of institutional implementation that could be adapted in Ukraine, taking into account the country's specific security context, as illustrated in more detail in Fig. 1.3.

ENISA plays a central coordinating and expert-analytical role, carrying out threat analysis and developing technical recommendations for the implementation of NIS2 (in particular the 'NIS2 Technical Implementation Guidance' of June 2025), conducts maturity assessments of critical infrastructure sectors (the annual ENISA NIS360 report, 2025) and publishes the annual ENISA Threat Landscape report.

According to the 2025 edition, which covers the period from July 2024 to June 2025, the agency analysed 4,875 verified incidents. Among the trends in the current EU cyber-threat landscape, ransomware attacks occupy a prominent place; ENISA identifies them as one of the most significant cyber-threats to the European Union. During 2024–2025, the ransomware ecosystem was characterised by further fragmentation, the emergence of new strains and Ransomware-as-a-Service (RaaS) models, occurring, in particular, against a backdrop of large-scale law enforcement operations and intensified internal competition between cybercriminal groups. According to ENISA, 82 variants of ransomware were recorded as having been used against organisations in EU Member States during the period under review (ENISA, 2025).



Note: the diagram illustrates the key coordination mechanisms, rather than a complete list of all EU institutions in the field of cybersecurity.

Fig. 1.3. Institutional framework for information security in the European Union

Source: compiled by the author based on Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2019/881 (Cybersecurity Act), Regulation (EU, Euratom) 2023/2841, the EU Council Recommendation of June 2025 on the EU Cyber Blueprint, and ENISA materials.

At the same time, the use of artificial intelligence technologies in social engineering is on the rise: large language models are being used to create more convincing phishing messages and to automate such attacks. ENISA views the proliferation of artificial intelligence not only as a factor in the scaling up of traditional cyber threats, but also as a source of new vulnerabilities in the digital environment (ENISA, 2025).

Another notable trend is the convergence of different categories of cyber-threat actors: cybercriminal, hacktivist and state-affiliated groups, which manifests itself in the mutual use of tools, infrastructure, tactics, techniques and procedures. ENISA, in particular, has documented the use of ransomware by pro-Russian hacktivist groups. A telling example is CyberVolk, whose activities ENISA characterises as serving Russian interests; since May 2024, the group has used and promoted several variants of ransomware, including AzzaSec, HexaLocker, Parano, LockBit and Chaos (ENISA, 2025).

Alongside monitoring and assessing cyber threats, ENISA also places a strong emphasis on developing human capital and operational readiness in the field of cybersecurity. The European Cybersecurity Skills Framework (ECSF) establishes a common approach to defining the professional roles, competencies, knowledge and skills of specialists, whilst the pan-European Cyber Europe exercises are designed to practise responses to large-scale cyber incidents, identify gaps in procedures and enhance individual and collective capacity for cyber crisis management (ENISA, 2022; ENISA, 2024). Thus, ENISA's toolkit combines analytical and regulatory-methodological mechanisms with the development of professional competencies, operational readiness and cyber resilience at EU and Member State level. Such a system ensures a seamless transition from the detection and technical handling of cyber incidents to the coordination of crisis response and the formulation of strategic decisions. Importantly, for Ukraine in particular, this approach is of interest not as a model to be mechanically replicated, but as an institutional benchmark for further aligning the national cybersecurity system with EU mechanisms, taking into account the specific nature of the security environment and established practices for countering cyber threats.

By examining the technical level of information security in the EU, it is worth noting that the CSIRTs Network, which brings together representatives of incident response teams designated by Member States, as well as CERT-EU, facilitates technical and operational cooperation, the exchange of information on cyber incidents, threats, risks and vulnerabilities, and the coordination of cross-border responses. As a member of the CSIRTs Network, CERT-EU performs specialised functions in

responding to cyber incidents within EU institutions, bodies, offices and agencies. This structure ensures a direct link between national response teams and the institutional framework of the European Union.

At the operational level, the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) plays a decisive role; its functional purpose is the coordinated management of large-scale cyber incidents and crises. Its operations ensure the development of a shared situational awareness, the coordination of Member States' operational actions, and support for decision-making at the political level. The interaction between EU-CyCLONe and the CSIRTs Network creates a mechanism for transitioning from a technical response to an incident to operational coordination should the incident escalate.

At the strategic/political level, the NIS Cooperation Group plays a key role, ensuring strategic cooperation between Member States, the exchange of information and best practices, and facilitating the consistent implementation of the NIS2 requirements. It is at this level that the outcomes of technical and operational responses are transformed into strategic guidelines, recommendations and approaches for the further development of the EU's common cybersecurity policy. At the same time, the functioning of the multi-level institutional framework for cybersecurity coordination established at EU level does not entail the standardisation of national institutional models. At Union level, a system of cooperation between Member States, EU institutions, bodies and agencies has been established, covering the technical, operational and political levels of response to large-scale cyber incidents and crises (Council of the European Union, 2025). A common regulatory framework sets out basic requirements, mechanisms for cooperation and coordination, as well as requirements for national cybersecurity capabilities, whilst the specific organisational arrangements for their implementation are determined by the Member States. NIS2, in particular, requires each Member State to adopt a national cybersecurity strategy, designate one or more competent authorities, a single point of contact, bodies responsible for managing large-scale cyber incidents and crises, and one or more CSIRTs (European Parliament & Council of the European Union, 2022). At the same time, the Directive does not prescribe a single organisational model for these

institutions: Member States determine their structure and the distribution of powers independently, within the established requirements. As a result, the EU's common legal and coordination framework coexists with a diversity of national governance architectures.

A comparative analysis shows that Member States implement common requirements through distinct governance models, shaped by the characteristics of their political systems, the historical development of their institutions, the security environment and administrative practices. Differences can be observed both in the degree of centralisation of cybersecurity governance and in the distribution of powers amongst competent authorities, sectoral regulators and incident response teams. The existence of such differences is also confirmed by the implementation of NIS2, under which Member States designate their own competent authorities and organisational mechanisms within the framework of a common regulatory and legal framework.

Considering the specific features of information security in the European Union, it is worth examining the particular characteristics of the Member States' national cybersecurity models, as it is at the national level that pan-European requirements are given concrete institutional and organisational form. The selection of countries for comparative analysis was based on the principle of maximum variation in institutional structure, provided that they operate within the EU's common legal framework in the field of information and cybersecurity. Four national models were selected for the study, representing distinct approaches to the organisation of cybersecurity and incorporating various institutional solutions that are potentially relevant to Ukraine.

Estonia represents a centrally coordinated but technologically decentralised model, shaped by a high level of state digitalisation and significant practical experience in countering large-scale cyber-attacks. Institutional coordination of cybersecurity is centred primarily within the RIA and its National Cyber Security Centre (NCSC-EE), whilst X-tee/X-Road functions as a distributed environment for secure data exchange between information systems (Information System Authority [RIA], n.d.-a, n.d.-b). Its experience has a direct technological counterpart in Ukraine: the 'Trembita' system for the electronic interaction of state information resources was created on the basis of

technological solutions derived from the Estonian X-Road (e-Governance Academy, 2017).

Germany is characterised by a federal-sectoral model, which combines the coordinating role of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), multi-level interaction between the federal level and the Länder, and a system of sectoral standards for the protection of critical infrastructure (Federal Office for Information Security [BSI], n.d.-a, n.d.-b).

France demonstrates a more centralised state-security model with a leading role for the National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information, ANSSI), which is the national authority in the field of cybersecurity and cyber defence and coordinates the state's defence against cyber-attacks (Agence nationale de la sécurité des systèmes d'information [ANSSI], n.d.-a). The French approach is also characterised by a strong emphasis on strategic autonomy, the protection of critical information systems and the development of trusted digital and cloud services; in particular, the SecNumCloud certification sets high technical, operational and legal requirements for cloud services intended to handle sensitive data (ANSSI, n.d.-b).

Poland represents a multi-level, sectorally coordinated model of a Central and Eastern European state, whose institutional development has taken place in the context of European integration and the subsequent adaptation of the national cybersecurity system to EU requirements. Poland's experience is of particular interest to Ukraine given the combination of a post-socialist institutional legacy, European integration and current security challenges. Poland has been a member of the EU since 1 May 2004 (European Union, 2004), and in 2026 the Act on the National Cybersecurity System (KSC) was amended to implement the requirements of NIS2; the relevant amendment came into force on 3 April 2026 (Ministry of Digital Affairs of Poland, 2026).

The comparison of these models is carried out using a single analytical framework: the institutional prerequisites for the development of the model, the regulatory and legal framework, the key competent authorities and organisational architecture, strengths and institutional constraints, as well as elements relevant to Ukraine. The application of a unified system of criteria ensures the methodological

comparability of national models and makes it possible to identify not a universal ‘best’ model, but rather those institutional solutions that can be taken into account in the further development of Ukraine’s cybersecurity system.

The Estonian model of cybersecurity and digital resilience was shaped to a large extent by experiences of crisis. In April–May 2007, against the backdrop of a political conflict between Estonia and Russia over the relocation of a monument to a Soviet soldier in Tallinn, Estonia’s digital infrastructure was subjected to a large-scale campaign of cyber-attacks. Over a period of 22 days, DDoS attacks targeted the websites of government institutions, the media and the private sector; some attacks also affected online banking and critical network services (Information System Authority [RIA], 2017; Ottis, 2008). The political motivation behind the attacks and their link to the wider conflict surrounding the relocation of the monument are well documented; however, unequivocally attributing these attacks to a specific state remained problematic (NATO, 2007; Ottis, 2008). These events became one of the best-known early examples of a large-scale, politically motivated cyberattack against a state’s digital infrastructure and had a significant impact on the subsequent development of cybersecurity policy in Estonia and NATO.

Meanwhile, the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was not a direct consequence of the 2007 attacks: Estonia proposed the concept to NATO as early as 2004; it was approved in 2006, and the Centre itself was established in Tallinn on 14 May 2008; in October of that year, it received NATO accreditation and the status of an international military organisation (NATO CCDCOE, n.d.). At the same time, the 2007 attacks served as a pivotal catalyst, demonstrating to the Alliance the growing significance of cyber threats and prompting a strengthening of cyber defence policy (NATO, 2019).

The institutional core of the modern Estonian model is the Estonian Information System Authority (Riigi Infosüsteemi Amet, RIA), which coordinates the development and administration of state information systems, ensures their interoperability, organises activities in the field of information security, and responds to incidents in Estonian computer networks (Information System Authority [RIA], 2026). The Estonian National Cyber Security Centre (NCSC-EE) operates within the RIA

structure, whose tasks include round-the-clock monitoring of cyberspace, incident response, protection of critical infrastructure, analysis of cyber threats, crisis management, conducting exercises and developing information security standards (RIA, 2026b).

The technological foundation of the digital state is the X-tee data exchange platform, which is based on X-Road technology. Its architecture is based on a distributed model: information is not stored in a single centralised database but is exchanged between participants' information systems via standardised and secure interaction mechanisms. As of 2026, over 4,500 data exchange services are available via X-tee, with the number of requests standing at around 13 million per day (RIA, 2026). Estonia's well-developed digital infrastructure has enabled the country to achieve the full digitalisation of public services: since December 2024, all the country's public services have been available in electronic format (e-Estonia, 2025).

The concept of a "data embassy" has proved to be an important institutional and technological solution. In fact, on 20 June 2017, Estonia and Luxembourg signed an agreement on the hosting of Estonian data and information systems in Luxembourg's national data centre with the aim of ensuring the country's digital continuity (Government of Estonia, 2017). The project provided for the backup of ten strategically important datasets, including the electronic court system, the State Treasury, the land and commercial registers, the population register, the tax register, identity documents, the cadastral register and the pension register (e-Estonia, n.d.). Legally, the 'digital embassy' is not a diplomatic mission in the traditional sense. Its special legal status is defined by an intergovernmental agreement, which ensures the immunity and protection of Estonian data and information systems hosted in Luxembourg (Riigikogu, 2018). This model aims to ensure the state's digital continuity, that is, the ability to preserve critical data and maintain the functioning of state information systems even in the event of the cessation or disruption of data centre operations within Estonia (Riigikogu, 2018).

Another key component of the Estonian model is the development of public practices in the use of the state's digital tools. Online voting was first introduced in the 2005 local elections and in the 2007 parliamentary elections (Elections in Estonia,

n.d.). The development of e-voting, alongside digital identification, electronic signatures and inter-agency data exchange, has heightened the demands on the reliability and security of the state's digital infrastructure.

The particular relevance of Estonia's experience for Ukraine is confirmed by the direct transfer of technology relating to solutions in the field of inter-agency data exchange. On 26 October 2017, as part of the EGOV4UKRAINE programme, documentation and rights were transferred to the State Agency for Electronic Governance of Ukraine to begin the implementation of the "Trembita" interoperability system, based on the Estonian X-Road (e-Governance Academy, 2017). Subsequently, "Trembita" became one of the key infrastructure components for secure data exchange between state registers and the development of digital public services in Ukraine (e-Governance Academy, 2026).

An analysis of the advantages of the Estonian model for ensuring information security highlights the following strengths. Firstly, the distributed architecture of X-tee/X-Road minimises the risk of a single point of failure: data exchange takes place directly between the participants' information systems, whilst the redundancy of Security Servers ensures service availability in the event of individual components failing (Nordic Institute for Interoperability Solutions, 2025). Secondly, security mechanisms are integrated directly into the data exchange architecture and cover authentication, authorisation, encryption, digital signing and transaction logging, in line with the "security by design" principle (Nordic Institute for Interoperability Solutions, 2025). This was also facilitated by the "no-legacy culture" characteristic of the development of the Estonian digital state, which made it possible to build digital infrastructure without the significant burden of legacy information systems (OECD, 2021). Thirdly, the model relies on a mature system of digital public administration and the reuse of shared infrastructure components, ensuring a high level of interoperability among public information resources (OECD, 2026). Fourthly, the Estonian model is characterised by a significant demonstration effect and the international dissemination of its institutional and technological solutions, one example of which is the adaptation of X-Road technology during the creation of the Ukrainian "Trembita" system (X-Road Security Architecture, 2023).

At the same time, a critical analysis of the Estonian model reveals a series of significant limitations. Firstly, the small domestic labour market exacerbates the problem of staffing for cybersecurity: Estonia's current Cybersecurity Strategy explicitly identifies a shortage of qualified specialists as one of the challenges to the development of national cybersecurity capabilities (Ministry of Economic Affairs and Communications, 2024). The significance of this problem is growing against the backdrop of a steady increase in the number of cyber incidents and the expanding range of entities subject to cybersecurity requirements (Information System Authority, 2026). Secondly, despite the distributed nature of X-tee, its operation depends on a variety of shared trust components and service infrastructure. This creates a risk of simultaneous disruption to the availability of a set of services in the event of failures in shared infrastructure components, as demonstrated, in fact, by the incident involving the X-tee timestamping service in 2026 (Information System Authority, 2026). Thirdly, the effectiveness of the Estonian model is largely linked to the specific trajectory of the digital state's development and the opportunity to build it following the restoration of independence according to the "no-legacy" principle, the high level of uptake of e-services, and the established practice of their everyday use by the population. This limits the scope for mechanically transferring the Estonian model to states with a different institutional structure and necessitates the adaptation of its individual elements to the national administrative and security environment (OECD, 2021).

The German model for ensuring information and cyber security is largely centred on the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), which began operations on 1 January 1991 and is a federal agency operating under the Federal Ministry of the Interior. In accordance with the current legislative framework, the BSI-Gesetz, the BSI acts as the central authority for information security at the national level (Federal Republic of Germany, 2025; Federal Office for Information Security [BSI], n.d.-a). The BSI develops standards and methodological approaches to information security, in particular IT-Grundschutz; certifies IT products and systems; ensures the operation of CERT-Bund and the National IT Situation Centre; and produces a nationwide assessment of the state of cyber security (BSI, n.d. -b, n.d.-c). After the NIS2 Implementation Act came into

force, the BSI assumed the role of the national contact point and central coordinating body, as well as the primary supervisory authority for important and particularly important entities, whilst cooperating with sectoral regulators, in particular the Bundesnetzagentur and BaFin (Federal Republic of Germany, 2025).

An essential element of the German model is the critical infrastructure protection regime (Kritische Infrastrukturen, KRITIS), which is traditionally based on a sectoral approach and quantitative threshold criteria. Prior to the reforms of 2025-2026, the national KRITIS model and the scope of regulation under the BSI-Gesetz did not fully coincide: for example, the ‘media and culture’ and “government and administration” sectors were part of the broader national KRITIS concept but were not fully covered by the previous BSI-KritisV regime (BSI, 2023). Following the reform, the current KRITIS-Dachgesetz defines ten sectors of critical services: energy; transport and logistics; finance; social insurance and basic services provided by employment centres; healthcare; water supply; food; information technology and telecommunications; the space sector; and household waste management (Federal Republic of Germany, 2026). The identification of critical facilities remains linked to facility categories and threshold values; if the relevant threshold is reached or exceeded, a specific installation or infrastructure facility is deemed critical, and its operator assumes the obligations laid down by law. Meanwhile, until the new subordinate legislation, the Kritisverordnung, comes into force, the relevant transitional provisions of the previous regime remain in force (Federal Republic of Germany, 2025, 2026).

The legal framework of the German model was developed in stages. The first Act on the Enhancement of Information System Security (IT-Sicherheitsgesetz) came into force on 25 July 2015 and implemented special requirements for the protection of IT systems operated by critical infrastructure operators, in particular requirements regarding the implementation of state-of-the-art security measures and the reporting of significant IT incidents (BSI, 2016).

The second version – the IT Security Act 2.0, came into force in May 2021 – expanded the scope of regulated entities, introduced the category of ‘undertakings of particular public interest’ (Unternehmen im besonderen öffentlichen Interesse, UBI) and explicitly required KRITIS operators to use attack detection systems. Operators

were required to provide the BSI with confirmation of the implementation of such systems for the first time by 1 May 2023 (BSI, 2021, 2023).

The next stage in the development of the regulatory framework relates to the implementation of the European NIS2 and CER Directives; the NIS-2-Umsetzungsgesetz came into force on 6 December 2025, i.e., more than a year after the transposition deadline set by NIS2 – 17 October 2024. The Act significantly expanded the scope of regulation and enshrined in German law the categories of important and particularly important entities, as well as updated requirements regarding cyber risk management, incident reporting and state supervision (BSI, 2025; Federal Republic of Germany, 2025). At the same time, the KRITIS-Dachgesetz, aimed at implementing Directive (EU) 2022/2557 on the resilience of critical entities (CER), came into force on 17 March 2026. The Act established, for the first time at the federal level, a unified cross-sectoral legal framework for the physical resilience of critical infrastructure, providing for the identification of critical facilities, the conduct of risk analysis and risk assessment, the implementation of resilience measures, the preparation of resilience plans, and the reporting of significant incidents. However, the specific details of certain cross-sectoral minimum requirements are to be set out in subordinate legislation, some of which, as of September 2026, are still at the drafting and consultation stage (KRITIS-DachG, BGBl. 2026 I No. 66; Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2026).

Thus, the German experience demonstrates that the implementation of comprehensive European regulation on cybersecurity and the resilience of critical infrastructure may be accompanied by significant delays, even in the presence of a well-developed institutional and regulatory framework.

Examining the advantages of the model, we can note that the concentration of technical expertise within a single specialised body (the BSI) ensures the high quality and consistency of national standards applicable across the entire federation. In addition, a sector-specific approach with clear quantitative thresholds (the KRITIS Regulation) provides businesses with relative legal certainty regarding their status as regulated entities. It is also worth drawing attention to the federal structure of the state, which creates the institutional conditions for the system to function effectively within

a large economy, whilst at the same time making it possible to avoid excessive centralisation of management decisions.

Despite the BSI's high level of institutional and technical capacity, one of the challenges facing the German model remains the complexity of the regulatory framework in the field of information and cyber security. This is shaped by the provisions of the BSI Act, legislation on the implementation of NIS2, the KRITIS Framework Act, as well as sector-specific regulations and special requirements for operators of critical infrastructure. Following the implementation of NIS2, the scope of regulation has expanded significantly: according to federal government estimates, the new requirements now apply to more than 30,000 entities, up from approximately 4,500. At the same time, the government estimated the one-off costs to businesses associated with complying with the new requirements at approximately €2.2 billion, and the annual costs at €2.3 billion. During the legislative process, the German Federal Council (Bundesrat) specifically emphasised the need to improve the practical feasibility of the regulation, reduce the bureaucratic burden and enhance cooperation between the federal and state levels. Consequently, the high level of regulatory detail, whilst ensuring the formalisation of cybersecurity requirements, simultaneously increases organisational and compliance costs for regulated entities (Deutscher Bundestag, 2025a; Deutscher Bundestag, 2025b).

Another challenge is the time taken to adapt national legislation to the new EU requirements. Directive (EU) 2022/2555 (NIS2) set a transposition deadline of 17 October 2024, whilst the German NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz did not come into force until 6 December 2025. In May 2025, the European Commission had already sent Germany a reasoned opinion regarding the incomplete transposition of the directive. A similar delay was observed with regard to Directive (EU) 2022/2557 on the resilience of critical entities (CER): whilst the transposition deadline was set for 17 October 2024, the KRITIS-Dachgesetz came into force on 17 March 2026; as early as July 2025, the European Commission sent Germany a reasoned opinion due to the failure to notify full transposition. The parallel delay in the implementation of two interrelated directives indicates the existence of time and procedural constraints in the mechanism for adapting German

legislation to dynamic changes in the EU legal framework (European Parliament and Council, 2022a, 2022b; European Commission, 2025a, 2025b; Deutscher Bundestag, 2026).

The next aspect relates to Germany's federal structure. The decentralised model creates opportunities to take regional specificities into account and to distribute responsibilities, but at the same time places greater demands on vertical coordination between federal and state authorities. A telling example in this context is the deliberations on the NIS2 legislation: the Bundesrat insisted on more explicit involvement of the Länder in the BSI's support mechanisms, ensuring their access to the information and reporting platform, and improving inter-level information exchange. The current BSI Act also explicitly provides for the BSI's coordinating role in cross-border cooperation between the relevant state authorities. Thus, federalism is both an advantage and a source of additional coordination costs: it reduces excessive centralisation of governance, yet requires well-developed mechanisms for the harmonisation of competences, information exchange and the standardisation of procedures between levels of government (Deutscher Bundestag, 2025a; BSIG, 2025).

An additional challenge is the transitional nature of the current critical infrastructure regulatory framework. Although the KRITIS-Dachgesetz came into force on 17 March 2026, as of September 2026, a range of the subordinate regulations it provides for are still at the drafting and approval stage. In particular, the German Federal Office for Civil Protection and Disaster Assistance (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK) notes that the implementing regulation defining critical facilities has not yet come into force, with the result that the new mechanism for registering operators is not yet fully operational; the development of methodological requirements for risk assessment and resilience plans is also ongoing. This situation creates a temporary gap between the entry into force of the framework law and the full functioning of all the instruments provided for therein (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2026).

A particular institutional challenge for the German model is ensuring public trust in cybersecurity bodies. A telling example in this context was the situation surrounding the former president of the BSI, Arne Schönbaum, who was suspended from his duties

in 2022 following public allegations of possible links to Russian organisations. Subsequent official investigations and court proceedings failed to confirm the existence of sufficient factual grounds for the allegations that he had knowingly maintained contacts with Russian intelligence services. This case demonstrated the importance of institutional trust, proper verification of security-sensitive information, and a clear distinction between reputational risks and confirmed threats to the resilience of the cybersecurity system (Deutscher Bundestag, 2023; Oberlandesgericht München, 2026).

Within the scope of the comparative analysis carried out, the French model of information security is characterised by a high degree of centralisation of its cybersecurity component and the close integration of information systems protection into the national security and defence framework. The central institution is the National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information, ANSSI), established in 2009 as the national authority in the field of information systems security. ANSSI reports organisationally to the General Secretariat for Defence and National Security (Secrétariat général de la défense et de la sécurité nationale, SGDSN), which, in turn, ensures the implementation of relevant state policy under the direction of the Prime Minister. ANSSI's functions include inter-ministerial coordination, the development of measures to protect information systems, the detection of and response to incidents, the conduct of audits, and the certification and accreditation of security products and services (Decree No. 2009-834, 2009).

A defining institutional feature of the French model is the separation of civilian, defence and military cyber functions. France's official doctrine is based on a division of responsibilities whereby the protection of information systems at the national level is entrusted to ANSSI, whilst the conduct of offensive military operations in cyberspace falls within the remit of the Ministry of the Armed Forces and the intelligence services. Within the military cyber defence system, a key role is played by the Cyber Defence Command (Commandement de la cyberdéfense, COMCYBER), established in May 2017 and reporting directly to the Chief of the Defence Staff. COMCYBER brings together the cyber defence forces of the Ministry of the Armed Forces and is responsible for planning and conducting defensive, offensive and

information operations in cyberspace. This model ensures an institutional separation between the civil protection of information systems and military operational activities, whilst maintaining mechanisms for their coordination (Ministère des Armées, 2023).

The practical effectiveness of this model was demonstrated during preparations for the 2024 Olympic and Paralympic Games in Paris. ANSSI played a leading role in ensuring the cyber security aspect of the event, coordinating the preparations of public and private entities, organisers and infrastructure operators for over two years. Despite significant media attention and an expanded attack surface for potential cyber-attacks, ANSSI assessed that the incidents recorded had no significant impact on the running of the Games; this was due to the effectiveness of the agency's prior preparation, training and cross-sectoral coordination (ANSSI, 2025).

An important component of the French system is the regime for the protection of operators of vital importance (opérateurs d'importance vitale, OIV). Unlike a purely economic approach, the classification of an entity as an OIV is linked to the significance of its activities for the state's defence and economic potential, national security, the state's ability to function, and the protection of the population's life and health. The regulatory framework for defining OIVs was established as early as Decree No. 2006-212 of 23 February 2006. Meanwhile, the 2013 Military Programming Act (Loi de programmation militaire, LPM) introduced a special cyber-security regime for their critical information systems: mandatory security rules, incident reporting, the possibility of conducting audits, and the application of special measures in the event of large-scale cyber crises. The relevant rules are laid down at the level of the Prime Minister, whilst ANSSI plays a key role in their implementation and in monitoring compliance (Décret No. 2006-212, 2006; Loi No. 2013-1168, 2013).

Another distinct element of the French approach to technological sovereignty is the SecNumCloud certification scheme, developed by ANSSI in 2016 to assess the security and reliability of cloud services. The current version of the SecNumCloud requirements combines technical, operational and legal criteria. Specifically, the supplier's registered office, central administration and principal place of business must be located in an EU Member State; the share of capital and voting rights directly or indirectly held by a single entity from outside the EU must not exceed 24 per cent, and

their combined share must not exceed 39 per cent. Certain requirements are designed to restrict access by non-European third parties to these customers and to mitigate risks associated with the application of extraterritorial legislation of third countries. Thus, SecNumCloud combines technical information protection with legal and organisational mechanisms to ensure control over critical cloud resources (ANSSI, 2022; ANSSI, 2026).

While analyzing the advantages of the French model for ensuring information security, it is worth emphasizing its key strengths first and foremost: firstly, a high level of institutional centralisation ensures unity in strategic leadership and inter-agency coordination in the field of information and cyber security. ANSSI's subordination to the General Secretariat for Defence and National Security under the Prime Minister creates the organisational framework for harmonising the actions of various state authorities within a single management system. In particular, the implementation of the state's digital systems security priorities for 2026–2027 involves monthly inter-agency monitoring involving the relevant departmental units under the auspices of ANSSI (Décret No. 2009-834, 2009; ANSSI, 2026).

Secondly, the direct institutional integration of ANSSI into the national security system ensures a high strategic status for issues relating to the protection of information systems and facilitates the concentration of specialised expertise. The expansion of the agency's functions was accompanied by a significant increase in staffing capacity: as of early 2025, ANSSI had 656 permanent staff, more than double the figure for 2021. At the same time, the further expansion of the regulatory framework, particularly in connection with NIS2, requires additional resources; it is therefore inappropriate to speak of its unconditional stability (Sénat, 2025).

Thirdly, the French model combines cybersecurity with ensuring technological and jurisdictional control over critical digital resources. The SecNumCloud certification scheme sets out not only technical requirements for cloud services, but also criteria regarding the provider's location, ownership structure and the protection of data from the application of extraterritorial legislation of third countries. This approach helps to mitigate jurisdictional risks and critical dependence on providers controlled by entities outside the EU (ANSSI, 2022). It is telling that in 2026 the

European Commission also introduced the Cloud Sovereignty Framework, which demonstrates the gradual spread of digital sovereignty principles at EU level (European Commission, 2026).

The institutional constraints of the French model are twofold. On the one hand, the concentration of coordination, regulatory and technical functions within ANSSI means that the effectiveness of the entire system depends on the agency having sufficient resources. The expansion of the regulatory environment resulting from the implementation of NIS2 and the shift from 500 OIV operators to 15,000 regulated entities creates a risk of institutional overload and is highlighted in parliamentary documents as a mismatch between ANSSI's expanded functions and the resources requested (Sénat, 2024; Sénat, 2025). On the other hand, the focus on digital sovereignty creates a structural trade-off between the level of protection and the competitiveness of the cloud services market: the stringent criteria of SecNumCloud narrow the pool of qualified providers and contribute to market segmentation, as directly noted by the Autorité de la concurrence (2023). Thus, striking a balance between technological sovereignty and the availability of innovative cloud solutions remains a significant challenge for the French model.

The Polish model serves as an important point of comparison for Ukraine, given Poland's experience of post-socialist transformation, its membership of the EU since 2004, and the consistent alignment of its national cybersecurity system with the EU acquis. This experience is particularly relevant for Ukraine, which is currently in the process of negotiating its accession to the EU.

The primary regulatory act is the Act of 5 July 2018 on the National Cybersecurity System (ustawa o Krajowym Systemie Cyberbezpieczeństwa, KSC), which transposed Directive (EU) 2016/1148 (NIS1). The institutional architecture of the KSC is based on a functional division of responsibilities between three national-level incident response teams – CSIRT NASK, CSIRT GOV and CSIRT MON – interacting with sectoral CSIRTs and competent authorities. Information and communication interaction between the system's participants is facilitated by the S46 platform, which is used for incident reporting, the exchange of information on cyber

threats and to support coordination within the KSC (Republic of Poland, 2018; Ministry of Digital Affairs, 2026a).

However, the implementation of NIS2 also demonstrated the complexity of operationally adapting national legislation to the new EU requirements. According to the transposition deadline set by the Directive – 17 October 2024 – the Polish Act amending the KSC was adopted on 23 January 2026 and came into force on 3 April 2026. The amendment has significantly expanded the scope of regulation: according to estimates by the Ministry of Digitalisation, the updated system may cover around 38,000 critical and important entities, including approximately 27,000 public sector entities. This demonstrates the significant scale of the organisational and regulatory transformation associated with the transition from NIS1 to NIS2 (Directive (EU) 2022/2555, 2022; Republic of Poland, 2026; Ministry of Digitalisation, 2026b).

When analysing the Polish model for ensuring information security, attention should first and foremost be paid to its key advantages. The functional separation of CSIRT NASK, CSIRT GOV and CSIRT MON ensures specialisation in responding to civilian, government and military cyber incidents, whilst the S46 system creates a unified environment for information exchange between KSC participants. Of particular interest to Ukraine is precisely this combination of specialised response channels with a centralised digital coordination platform, which enables inter-agency cooperation within the complex, multi-stakeholder institutional environment.

Meanwhile, the need for further strengthening of coordination is reflected in the Republic of Poland's Cybersecurity Strategy until 2029, approved by the Council of Ministers on 10 March 2026. This document provides for the progressive formation, based on the Joint Cyber Security Operations Centre (Polaczone Centrum Operacyjne Cyberbezpieczeństwa, PCOC), of a central coordinating body for the national cyber security system, as well as the further development of sectoral CSIRTs and the S46 system. This indicates a gradual transition from a predominantly decentralised coordination model towards strengthened centralised strategic and operational management (Council of Ministers, 2026; Ministry of Digital Affairs, 2026c).

The institutional limitations and challenges of the model are as follows: firstly, the transposition of NIS2 in Poland was delayed by approximately seventeen months:

although the deadline was set for 17 October 2024, the relevant amendments to the Act on the National Cybersecurity System did not come into force until 3 April 2026. This demonstrates that institutional integration into the EU legal framework does not preclude significant time and procedural delays in the transposition process (European Commission, 2025; Republic of Poland, 2026).

Secondly, the multi-stakeholder structure of the KSC, which brings together three national CSIRTs, sectoral CSIRTs and competent authorities, places greater demands on inter-agency coordination and a clear delineation of responsibilities. This risk is partially mitigated by the S46 system, which provides a centralised digital channel for incident reporting and automated routing of information. However, the phased implementation of the new NIS2 requirements up to 2027 prolongs the transition to the full operation of the updated system (Ministry of Digital Affairs, 2026; Republic of Poland, 2026).

A comparative analysis of four national models reveals that there is no single institutional model for information security within the EU. Common regulatory requirements are implemented through various national systems: centralised coordination with a distributed digital infrastructure in Estonia, a federal-sectoral model in Germany, a centralised model in France and a multi-stakeholder system in Poland (RIA, 2026; BSI, 2026; ANSSI, 2026; Ministry of Digital Affairs, 2026a). Specifically, Estonia's X-tee ensures secure data exchange between autonomous information systems without concentrating them in a single centralised database (RIA, 2026). The differences between the models reflect varying approaches to combining centralised management, functional specialisation, inter-agency coordination and the resilience of the information infrastructure. However, the experience of Germany and Poland illustrates that adapting national legislation to EU requirements can entail significant time and procedural costs, even where well-established national cybersecurity institutions are in place (European Commission, 2025; Ministry of Digitalisation, 2026b).

For Ukraine, the experience of the countries studied provides primarily a source of specific institutional solutions, rather than ready-made models to replicate. Estonia's experience is relevant in terms of a decentralised data-sharing infrastructure; Poland's,

in terms of multi-stakeholder coordination and the development of the KSC; France's, with regard to centralised strategic management; and Germany's, concerning the organisation of cooperation between the federal and state levels (RIA, 2026; Ministry of Digitalisation, 2026a; ANSSI, 2026; BSI, 2026). The Polish Cybersecurity Strategy up to 2029 further provides for enhanced coordination and the development of a national cybersecurity system (Ministry of Digitalisation, 2026c).

Consequently, instead of mechanically replicating a specific national model, it is advantageous for Ukraine to develop its own institutional architecture, taking into account the requirements of the EU acquis, the current security environment and existing administrative capacities, as set out in Table 1.3.

The legal framework for cybersecurity in Ukraine has been developed in stages, with a focus on strengthening institutional coordination and transitioning to risk-based protection mechanisms. The fundamental regulatory act is the Law of Ukraine 'On the Basic Principles of Ensuring Ukraine's Cybersecurity' No. 2163-VIII of 5 October 2017, which established the institutional framework for the national cybersecurity system and defined the powers of the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police, the Ministry of Defence and the General Staff of the Armed Forces of Ukraine, the intelligence agencies and the National Bank of Ukraine. Coordination functions were assigned to the National Cybersecurity Coordination Centre as a working body of the National Security and Defence Council of Ukraine. At that time, CERT-UA was already operating within the State Service for Special Communications; the legislation cemented its place in the national cyber incident response system (Verkhovna Rada of Ukraine, 2017; CERT-UA, 2026).

A new stage in the development of the regulatory framework is linked to the adoption of Law of Ukraine No. 4336-IX of 27 March 2025, which came into force in April 2025 and implemented several key principles of NIS2.

Table 1.3.

Comparative characteristics of national models for ensuring information security

Country	Type of institutional model	Key institutions	Characteristic features of the model	Institutional constraints and challenges	Elements potentially relevant to Ukraine
Estonia	Centralised coordination within a decentralised digital infrastructure	RIA / NCSC-EE; CERT-EE	X-tee's distributed architecture; absence of a single centralised database; integration of cybersecurity with the functioning of the e-government; round-the-clock monitoring and incident response.	High dependence of government and societal processes on the continuity of digital services; the need to constantly adapt security mechanisms to the growing number and complexity of cyber incidents	Distributed architecture for government data exchange; the NCSC/CERT model; protection of critical information infrastructure; principles of secure inter-agency data exchange.
Germany	Federal, multi-level, sector-specific	BSI; cooperation with state authorities and sectoral regulators	Federal Technical Centre; B3S system of sectoral standards; specific regulation of critical infrastructure; 24/7 National IT Situation Centre.	The complexity of multi-level coordination and the regulatory environment; a lengthy process of adapting to EU legislation. The European Commission has noted Germany's incomplete transposition.	Federal-regional coordination; sectoral standards; critical infrastructure protection system; monitoring, audit and response mechanisms.
France	Centralised, state-coordinated	ANSSI	Concentration of significant regulatory and technical functions within ANSSI; a special protection regime for OIVs and their information systems; a system for classifying trusted solutions, in particular SecNumCloud.	A significant number of specific requirements for the most sensitive information systems and qualification procedures. A particular current challenge is the delay in the full transposition of NIS2: the European Commission has referred the case concerning France to the Court of Justice of the European Union due to the failure to notify full transposition.	Centralised coordination of the protection of critical information systems; the qualification of trusted cloud services; mechanisms for the protection of operators of strategic importance.
Poland	Multi-stakeholder, inter-ministerial and sector-specific	Ministry of Digital Affairs; CSIRT NASK; CSIRT GOV; CSIRT MON	Functional specialisation of the three national CSIRTs; integration of sectoral competent authorities; use of S46 as a shared information and communication environment for the KSC.	The large number of bodies involved highlights the importance of coordination and a clear delineation of responsibilities; in 2026–2027, the system is undergoing the practical implementation of the new NIS2 requirements, the registration of entities and their connection to S46.	Division of functions amongst specialised CSIRTs; a single information-sharing platform, S46; experience of organisational adaptation of the national system to NIS2.

Source: compiled by the authors based on official materials from the Information System Authority of Estonia (RIA), the Federal Office for Information Security (BSI), the French Cybersecurity Agency (ANSSI), the Ministry of Digital Affairs of the Republic of Poland and the national legislation of the countries under study (RIA, 2026; BSI, 2026; ANSSI, 2026;

The Act provided for the establishment of departments and the creation of cybersecurity management posts within public authorities, the designation of responsible persons at critical information infrastructure sites, the development of national response systems and mechanisms for exchanging information on cyber incidents, as well as a shift from a predominantly permissive model of cybersecurity to the authorisation of systems and risk-based management of security throughout their lifecycle (Verkhovna Rada of Ukraine, 2025; State Special Communications Service, 2025).

The need for such a transformation is heightened by the increasing intensity of cyber threats in the context of war. According to CERT-UA, the number of cyber incidents recorded rose from 2,194 in 2022 to 4,315 in 2024, representing an increase of almost 70 per cent compared with 2023. At the same time, these figures should not be directly linked to the effect of Law No. 4336-IX, as the trend described had already taken shape before the law came into force (State Special Communications Service, 2025).

A comparison with the models of EU Member States indicates that the Ukrainian system is gradually aligning with European principles of multi-level response, the division of responsibilities among competent authorities, and risk-based management. In its Ukraine Report 2025, the European Commission noted a significant update to legislation and the creation of a unified national cyber incident response system, whilst emphasising that a set of provisions of the *acquis* still require full implementation to achieve compliance with NIS2 (European Commission, 2025).

Further development of the regulatory framework has already partially resolved certain discrepancies. Resolution No. 1533 of the Cabinet of Ministers of Ukraine, dated 26 November 2025, introduced reporting deadlines for significant cyber incidents, similar to those set out in Article 23 of NIS2: an initial report must be submitted within 24 hours, a progress report within 72 hours, and a final report within one month. Furthermore, Ukraine has in place a procedure for classifying facilities as critical infrastructure and maintains a Register of Critical Infrastructure Facilities;

therefore, their establishment should no longer be regarded as an unfulfilled harmonisation task (Cabinet of Ministers of Ukraine, 2025; 2026).

Consequently, the main areas for further alignment with the EU acquis remain the completion of the implementation of the provisions of NIS2, the further refinement of mechanisms for cooperation between competent authorities and the CSIRT, and the completion of the personal data protection reform. The latter area remains particularly relevant: the European Commission has noted that the Ukrainian personal data protection system does not sufficiently comply with the EU acquis, whilst Bill No. 8153 ‘On the Protection of Personal Data’ was still undergoing consideration in the Verkhovna Rada of Ukraine as of September 2026 (European Commission, 2025; Verkhovna Rada of Ukraine, 2026).

Special attention should be paid to harmonisation in the field of personal data protection, which is functionally linked to ensuring information and cyber security. Against the backdrop of a significant overhaul of cyber security legislation, the current Law of Ukraine ‘On the Protection of Personal Data’ of 2010 does not ensure full compliance with the current EU acquis. In its Ukraine Report 2025, the European Commission noted the inadequacy of the current regulatory and institutional framework for personal data protection and the lack of progress in aligning it with the acquis, emphasising the need to adopt new legislation. Draft Law No. 8153, aimed at modernising this area in line with the GDPR, was, as of September 2026, being prepared for its second reading; in parallel, Draft Law No. 6177 on the establishment of a specialised supervisory authority remains under consideration (European Commission, 2025; Verkhovna Rada of Ukraine, 2026a, 2026b). The GDPR, unlike the previous Directive 95/46/EC, establishes an expanded system of data subjects’ rights, the role of a data protection officer for certain categories of controllers and processors, and significantly stricter sanction mechanisms (European Parliament and Council, 2016).

The practical dimension of alignment with the EU acquis is supported by the regular Ukraine–EU Cyber Dialogue. The fourth round, held in Kyiv on 16 October 2025, covered the implementation of NIS2, the protection of critical infrastructure, the digital component of Ukraine’s Plan, the implementation of EU cybersecurity tools for

5G networks, and cyber defence issues. This format ensures a combination of regulatory alignment with operational and institutional cooperation in the field of cyber resilience (European Commission, 2025b).

Further harmonisation is also integrated into the negotiation process regarding Ukraine's accession to the EU; on 15 June 2026, the first negotiation cluster, "Fundamentals", was opened, whilst Chapter 10, "Digital Transformation and Media", falls under Cluster 3, "Competitiveness and Inclusive Growth"; its bilateral screening took place from 31 March to 1 April 2025 and covered, in particular, cybersecurity, electronic identification and trust services, open data, the DSA, the DMA and P2B. As of September 2026, Cluster 3 has not yet been opened for formal negotiations; Clusters 1 and 6 are open. According to the European Commission's assessment, Ukraine is at a level between moderate and good in terms of preparedness under Chapter 10, whilst some provisions of NIS2, the DSA, the DMA, P2B and other acts of the *acquis* still require further implementation (European Commission, 2025a).

Consequently, the current trend indicates a gradual convergence of the Ukrainian information security system with the EU's legal and institutional framework; however, the completion of this process requires the further implementation of NIS2, the modernisation of legislation on the protection of personal data, and the completion of the adaptation of regulations governing digital services and trust services.

Ensuring information security in the context of digital transformation is determined not only by the quality of the regulatory framework, but also by the state's institutional capacity to ensure its practical implementation. The analysis carried out has shown that the common EU regulatory framework, comprising the GDPR, NIS2, CRA, DSA, Cybersecurity Act and DGA, is implemented through various national institutional models, the effectiveness of which depends on coordination mechanisms, the distribution of powers, staffing capacity and readiness to respond to cyber threats. Consequently, the further harmonisation of Ukrainian legislation with the EU *acquis* should envisage not only regulatory alignment but also the development of Ukraine's own institutional architecture for information security, taking into account European experience, national administrative capacities and the specific nature of the security environment in the context of war and post-war reconstruction.

Perspective areas for further research in this field include the quantitative assessment of the relationship between the level of centralisation of the institutional system and the speed of response to cyber incidents; a comparative analysis of public–private partnership models for the protection of critical information infrastructure; research into mechanisms for inter-agency coordination in the context of hybrid threats; and an assessment of the economic efficiency of investments in the development of professional competencies in the field of information security as a component of strengthening Ukraine’s human capital during wartime and in the post-war period.

REFERENCES FOR SUBSECTION 1.3

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (*General Data Protection Regulation*). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (*NIS2 Directive*). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
3. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 (*Digital Services Act*). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
4. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 (*Cyber Resilience Act*). URL: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>
5. ENISA Threat Landscape 2025. *European Union Agency for Cybersecurity*, 2025. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
6. European Commission. *Digital Strategy*. URL: https://commission.europa.eu/index_en
7. On the Basic Principles of Ensuring Cybersecurity of Ukraine: *Law of Ukraine of 5 October 2017 No. 2163-VIII*. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
8. On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities: *Law of Ukraine of 27 March 2025 No. 4336-IX*. URL: <https://zakon.rada.gov.ua/laws/show/4336-20>
9. State Service of Special Communications and Information Protection of Ukraine. *Ukraine Is Transforming Its Cybersecurity System in Line with European Standards. Cabinet of Ministers of Ukraine*, 2026. URL: <https://www.kmu.gov.ua/news/derzhspetsviazku-ukraina-transformuie-systemu-kiberbezpeky-za-ievropeiskymy-standartamy>
10. Ukraine and the EU Deepen Cybersecurity Cooperation during the 4th Round of the Cyber Dialogue. *Delegation of the European Union to Ukraine*, 2025. URL: <https://eeas.europa.eu/delegations/ukraine/>
11. X-Road data exchange platform. *Republic of Estonia Information System Authority (RIA)*. URL: <https://e-estonia.com/programme/e-estonia-programme-on-x-road/>

12. Estonia to establish the world's first data embassy in Luxembourg. *Government of the Republic of Estonia*, 2017. URL: <https://valitsus.ee/en/news/estonia-establish-worlds-first-data-embassy-luxembourg>
13. Federal Office for Information Security (BSI). *KRITIS-Verordnung, IT-Sicherheitsgesetz 2.0*. URL: <https://www.bsi.bund.de>
14. Agence nationale de la sécurité des systèmes d'information (ANSSI). *Qualification SecNumCloud*. URL: <https://cyber.gouv.fr>
15. Ministry of Digital Affairs of Poland. (2026, April 14). Amendment to the Act on the national cybersecurity system. <https://www.gov.pl/web/baza-wiedzy/nowelizator-ustawy-o-krajowych-systemie-cyberbezpieczenstwa>
16. Council of the European Union. (2025). Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management (C/2025/3445). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/C/2025/3445/oj/eng>
17. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union, L 333, 80-152. <https://eur-lex.europa.eu/eli/dii/2022/2555/oj/eng>
18. Information System Authority. (2017, April 26). *Head of CERT-EE: Estonia's capability to manage cyber crises has improved significantly in 10 years*, <https://ria.ee/en/news/head-cert-ee-estonias-capability-manage-cyber-crises-has-improved-significantly-10-years>
19. NATO. (2007, May 23). *Press briefing*, <https://www.nato.int/en/news-and-events/events/transcripts/2007/05/23/press-briefing>
20. Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In D. Remenyi (Ed.), *Proceedings of the 7th European Conference on Information Warfare and Security* (pp. 163—168). Academic Conferences Limited. <https://www.etis.ee/portal/publications/display/c269960c-2e40-44b1-aa43-a7c62e9caaa6>
21. NATO Cooperative Cyber Defence Centre of Excellence, (n.d.). *About us*. <https://ccdcoe.org/about-us/>
22. Information System Authority. (2026). *Tasks and structure of the authority*. <https://www.ria.ee/en/authority-news-and-contact/authority-and-management/tasks-and-structure-authority>
23. Information System Authority, (n.d.). *National Cyber Security Centre NCSC-EE*. <https://www.ria.ee/en/cyber-security/national-cyber-security-centre-ncsc-ee>
24. Government of Estonia. (2017, June 20). *Estonia to establish the world's first data embassy in Luxembourg*, <https://www.valitsus.ee/en/news/estonia-establish-worlds-first-data-embassy-luxembourg>
25. e-Estonia. (n.d.). *Data embassy*. <https://e-estonia.com/wp-content/uploads/factsheet-data-embassy.pdf>
26. Elections in Estonia, (n.d.). *Statistics about Internet voting in Estonia*. <https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia>
27. Kriisa, K. (2025, January 27). *Estonia: 100% digital government services, with divorce as the final step*. e-Estonia. <https://e-estonia.com/estonia-100-digital-government-services/>
28. e-Governance Academy. (2017, October 26). *Ukraine to begin the implementation of interoperability system*, <https://ega.ee/ukraine-to-begin-the-implementation-of-interoperability-system/>
29. e-Governance Academy. (2026). *Трембіта - фундамент цифрової держави*. <https://ega.ee/uk/trembita/>

30. e-Governance Academy. (2017, October 26). *Ukraine to begin the implementation of interoperability system*, <https://ega.ee/ukraine-to-begin-the-implementation-of-interoperability-system/>
31. Information System Authority. (2026a, February 4). *Cyber security in Estonia: New records, old mistakes*, <https://www.ria.ee/en/news/cyber-security-estonia-new-records-old-mistakes>
32. Information System Authority. (2026b, July 6). *Situation in cyberspace - June 2026*. <https://ria.ee/en/situation-cyberspace-june-2026>
33. Ministry of Economic Affairs and Communications. (2024). *Cybersecurity strategy 2024-2030: "Cyber-conscious Estonia"*. Republic of Estonia. Cybersecurity Strategy 2024-2030 PDF
34. Nordic Institute for Interoperability Solutions. (2025). *X-Road security architecture* (Version 0.11, Technical Specification ARC-SEC). X-Road Documentation, <https://docs.x-road.global/Architecture/arc-sec/x-road-security-architecture.html>
35. Organisation for Economic Co-operation and Development. (2021). *The E-Leaders handbook on the governance of digital government*. OECD Publishing. <https://doi.org/10.1787/ac7f2531-en>
36. Organisation for Economic Co-operation and Development. (2026). *Digital government outlook 2026: From foundations to transformational impact*. OECD Publishing. <https://doi.org/10.1787/0496b2bc-en>
37. KRITIS Act of March 11, 2026 (BGBl. 2026 I No. 66), as amended by Article 8 of the Act of July 21, 2026 (BGBl. 2026 I No. 221). *KRITISDachG - Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen*.
38. Federal Office of Civil Protection and Disaster Assistance (BBK). (2026). *FAQ on the KRITIS Umbrella Act*. The BBK explains that the Act entered into force on March 17, 2026, but that implementing ordinances and cross-sectoral minimum requirements are still being drafted. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Strategien-und-rechtlicher-Rahmen/KRITISDachG/FAQ/faq_node.html?utm
39. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2026). *FAQ zum KRITIS- Dachgesetz*. BBK - FAQ zum KRITIS-Dachgesetz <https://www.bbk.bund.de/>.
40. Bundesministerium der Justiz. (2025). *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI- Gesetz — BSIg) vom 2. Dezember 2025* (BGBl. 2025 I Nr. 301). https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html
41. Bundesministerium der Justiz. (2026). *Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz - KRITISDachG) vom 11. März 2026* (BGBl. 2026 I Nr. 66). <https://www.gesetze-im-internet.de/kritisdachg/BJNR0420B0026.html>
42. Deutscher Bundestag. (2023). *Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU: Abberufung und Versetzung des früheren Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik Arne Schönbohm* (Drucksache 20/7366). <https://dserver.bundestag.de/btd/20/073/2007366.pdf>
43. Deutscher Bundestag. (2025). *Gesetz zur Informationssicherheit in der Bundesverwaltung* beschlossen, <https://www.bundestag.de/dokumente/textarchiv/2025/kw46-de-nis-2-1123138>
44. European Commission. (2025a, May 7). *Commission calls on 19 Member States to fully transpose the NIS2 Directive*, <https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive>

45. European Commission. (2025b, July 17). *July infringements package: Key decisions*. [Section on the transposition of Directive (EU) 2022/2557 on the resilience of critical entities]. https://luxembourg.representation.ec.europa.eu/actualites-et-evenements/actualites/july-infringements-package-key-decisions-2025-07-17_fr
46. European Parliament and Council of the European Union. (2022a). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union, L 333, 80-152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
47. European Parliament and Council of the European Union. (2022b). *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive)*. Official Journal of the European Union, L 333, 164-198. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
48. Agence nationale de la sécurité des systèmes d'information. (2026). *What we do*. <https://cyber.gouv.fr/en/aboirt-anssi/what-we-do/>
49. Bundesamt für Sicherheit in der Informationstechnik. (2026). *Bund-Länder-Zusammenarbeit*. https://www.bsi.bund.de/DE/Das-BSI/Organisation-und-Aufbau/Abteilungen-inkl-Organigramm/Bund-Laender-Zusammenarbeit/bund-laender-zusammenarbeit_node.html
50. Information System Authority. (2026). *Cyber Security in Estonia 2026*. <https://www.ria.ee/en/cyber-security-estonia-2026>
51. Information System Authority. (2026). *National Cyber Security Centre NCSC-EE*. <https://www.ria.ee/en/cyber-security/national-cyber-security-centre-ncsc-ee>
52. Ministerstwo Cyfryzacji. (2026). *System S46*. <https://www.gov.pl/web/system-s46/o-systemie-s46>
53. Oberlandesgericht München. (2026). *Endurteil vom 16.06.2026 - 18 U 217/25 Pre e: Erfolgreicher Eilantrag wegen Berichterstattung über angebliche Kontakte zu russischen Geheimdienstkreisen*. <https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2026-N-14114>
54. Agence nationale de la sécurité des systèmes d'information. (2022). *Prestataires de services d'informatique en nuage (SecNumCloud) : Référentiel d'exigences, version 3.2*. Premier ministre. <https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf>
55. Agence nationale de la sécurité des systèmes d'information. (2025). *ANSSI2024 annual review*. <https://cyber.gouv.fr/en/publications/annual-reviews/anssi-2024-annual-review/>
56. Agence nationale de la sécurité des systèmes d'information. (2026). *FAQ avant de se lancer dans la qualification SecNumCloud*. <https://cyber.gouv.fr/enjeux-technologiques/cloud/faq-qualification-secnumcloud/>
57. France. (2006). *Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale*. Journal officiel de la République française. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000634536>
58. France. (2009). *Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »*. Journal officiel de la République française. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000020828212>
59. France. (2013). *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, art. 22. Journal officiel de la République française. https://www.legifrance.gouv.fr/jorf/article_i/JORFARTI000028338907

60. Ministère des Armées et des Anciens combattants. (2023). *Et la cyberdéfense devint une priorité nationale*, <https://www.defense.gouv.fr/actualites/cyberdefense-devint-priorite-nationale>
61. Agence nationale de la sécurité des systèmes d'information. (2022). *Prestataires de services d'informatique en nuage (SecNumCloud): Référentiel d'exigences, version 3.2*. Premier ministre. <https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf>
62. Agence nationale de la sécurité des systèmes d'information. (2026). *Publication de la feuille de route des efforts prioritaires en matière de sécurité numérique de l'Etat 2026-2027*. <https://cyber.gouv.fr/actualites/feuille-de-route-des-efforts-prioritaires-en-matiere-de-securite-numerique-de-letat-2026-2027/>
63. Autorité de la concurrence. (2023). *Avis n° 23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage («cloud»)*, <https://www.autoritedelaconcurrence.fr/fr/article/lautorite-rend-son-avis-sur-le-fonctionnement-concurrentiel-du-secteur-du-cloud>
64. European Commission. (2026, June 1). *Sovereign Cloud Framework explained*. https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en
65. Sénat. (2024). *Projet de loi de finances pour 2023: Direction de l'action du Gouvernement - Coordination du travail gouvernemental*, <https://www.senat.fr/rap/a24-146-9/a24-146-91.html>
66. Sénat. (2025). *Projet de loi de finances pour 2026: Direction de l'action du Gouvernement*, <https://www.senat.fr/rap/125-139-39/125-139-393.html>
67. European Parliament and 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 (NIS2 Directive)*. Official Journal of the European Union, L 333, 80-152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
68. Ministerstwo Cyfryzacji. (2026a). *Czym jest System S46*. <https://www.gov.pl/web/system-s46/o-systemie-s46>
69. Ministerstwo Cyfryzacji. (2026b). *Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) - kogo obejmuje?* <https://www.gov.pl/web/cyfryzacja/novelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenia-ksc-kogo-obejmuje>
70. Ministerstwo Cyfryzacji. (2026c). *Nowa strategia cyberbezpieczeństwa. Polska wzmacnia ochronę przed cyberatakami*. <https://www.gov.pl/web/cyfryzacja/nowa-strategia-cyberbezpieczenia-polska-wzmacnia-ochrone-przed-cyberatakami>
71. Rada Ministrów. (2026). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej*. Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r., M.P. 2026 poz. 309. <https://monitorpolski.gov.pl/M2026000030901.pdf>
72. Republic of Poland. (2018). *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*. Dz.U. 2018 poz. 1560. <https://eli.gov.pl/eli/DU/2018/1560/ogl>
73. Republic of Poland. (2026). *Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*. Dz.U. 2026 poz. 252. <https://eli.gov.pl/eli/DU/2026/252/ogl>
74. Verkhovna Rada of Ukraine. (2017). *On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine of 5 October 2017 No. 2163-VIII*. Legislation of Ukraine Database. <https://zakon.rada.gov.ua/laws/show/2163-19>
75. Verkhovna Rada of Ukraine. (2022). *Draft Law on Personal Data Protection No. 8153 of 25 October 2022*. <https://itd.rada.gov.ua/billinfo/Bills/Card/40707>

76. Verkhovna Rada of Ukraine. (2025). On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities: *Law of Ukraine of 27 March 2025 No. 4336-IX*. Legislation of Ukraine Database, <https://zakon.rada.gov.ua/laws/show/4336-20>
77. State Service of Special Communications and Information Protection of Ukraine. (2025). Russian Cyber Operations: Analysis for the Second Half of 2024. CERT-UA, State Cyber Protection Centre.
78. European Commission. (2025). *Ukraine Report 2025*. Directorate-General for Enlargement and Eastern Neighbourhood, https://enlargement.ec.europa.eu/ukraine-report-2025_en
79. Cabinet of Ministers of Ukraine. (2020). Certain Issues Concerning Critical Infrastructure Facilities: *Resolution of the Cabinet of Ministers of Ukraine of 9 October 2020 No. 1109 (as amended)*. Legislation of Ukraine Database.
80. Cabinet of Ministers of Ukraine. (2023). On Approval of the Procedure for Maintaining the Register of Critical Infrastructure Facilities, Including Such Facilities in the Register, Accessing the Register and Providing Information Therefrom: Resolution of the Cabinet of Ministers of Ukraine of 28 April 2023 No. 415 (as amended in 2026). Legislation of Ukraine Database. <https://zakon.rada.gov.ua/go/415-2023-п>
81. Cabinet of Ministers of Ukraine. (2025). Certain Issues Concerning Response to Cyber Incidents, Cyberattacks and Cyber Threats: *Resolution of the Cabinet of Ministers of Ukraine of 26 November 2025 No. 1533*. Legislation of Ukraine Database, <https://zakon.rada.gov.ua/laws/show/1533-2025-n>
82. European Commission. (2025a). *Ukraine 2025 Report. Commission Staff Working Document SWD(2025) 759final*. European Commission.
83. European Commission. (2025b, October 18). *EU and Ukraine deepen cooperation on cyber security at 4th Cyber Dialogue*, <https://digital-strategy.ec.europa.eu/en/news/eu-and-ukraine-deepen-cooperation-cyber-security-4th-cyber-dialogue>
84. European Parliament and 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 (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1-88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
85. Council of the European Union. (2026, June 15). *EU and Ukraine open first accession negotiations cluster*, <https://www.consilium.europa.eu/en/press/press-releases/2026/06/15/eu-and-ukraine-open-first-accession-negotiations-cluster/>
86. Verkhovna Rada of Ukraine. (2010). On Personal Data Protection: *Law of Ukraine of 1 June 2010 No. 2297-VI*. Legislation of Ukraine Database. <https://zakon.rada.gov.ua/laws/show/2297-17>
87. Verkhovna Rada of Ukraine. (2026a). *Draft Law on Personal Data Protection No. 8153 of 25 October 2022*. <https://itd.rada.gov.ua/billinfo/Bills/Card/40707>
88. Verkhovna Rada of Ukraine. (2026b). *Draft Law on the National Commission for Personal Data Protection and Access to Public Information No. 6177 of 18 October 2021*. <https://itd.rada.gov.ua/billinfo/Bills/Card/38789>
89. Ministry of Digital Transformation of Ukraine. (2025, 1 April). The Next Stage of Ukraine's Accession to the EU: *Bilateral Screening Meeting in the Field of Digital Transformation and Media*. <https://thedigital.gov.ua/news/nastupniy-etap-vstupu-ukraini-do-es-dvostopoHHa-skrining-zustrich-u-sferi-tsifrovoi-transformatsii-ta-media>