

# Ukrainian Cybersecurity Legal Framework:

OVERVIEW AND ANALYSIS

April 2021





# Ukrainian Cybersecurity Legal Framework:

## Overview and Analysis

Lilia Oleksiuk\*

International Foundation for Electoral Systems



*This report was developed by the International Foundation for Electoral Systems (IFES) through the support of the United States Agency for International Development (USAID), Global Affairs Canada and UK aid. The opinions expressed herein are those of the author and do not necessarily reflect the views and opinions of the USAID, nor the governments of the United States, Canada, or the UK.*

\*IFES wishes to thank Thomas Chanussot, IFES Cybersecurity and Election Technology Advisor, for his review and input to this report



Ukrainian Cybersecurity Legal Framework: Overview and Analysis. Second edition.  
Copyright © 2021 International Foundation for Electoral Systems. All rights reserved.

This analysis was conducted over the course of 2020 and it reflects all major updates to the date of publication.

Permission Statement: No part of this publication may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without the written permission of IFES.

Requests for permission should include the following information:

- A description of the material for which permission to copy is desired.
- The purpose for which the copied material will be used and the manner in which it will be used.
- Your name, title, company or organization name, telephone number, fax number, email address, and mailing address.

Please send all requests for permission to:

International Foundation for Electoral Systems  
2011 Crystal Drive, 10th Floor  
Arlington, VA 22202  
Email: [editor@ifes.org](mailto:editor@ifes.org)  
Fax: 202.350.6701

# Content

<b>Preliminary Review</b> .....	7
<b>Introduction and Methodology</b> .....	9
<b>Obligations Defined by International Agreements and Other Documents in the Field of Cybersecurity</b> .....	10
Budapest Convention and Convention 108+ .....	11
EU Documents .....	12
Conclusions .....	15
<b>National Legislation</b> .....	16
National Security Strategy .....	19
Cybersecurity Strategy .....	20
Legislative Level. The Cybersecurity Law .....	23
Level of bylaws .....	26
Conclusions .....	29
Draft Laws .....	31
The draft law on Critical Infrastructure, new version .....	31
The draft law on Cloud Services (dated 16.06.2020 No. 2655) .....	33
The Law of Ukraine «On Electronic Communications» Number 1089-IX of December 16, 2020. Becomes law on January 1, 2022. ....	34
The draft law on the National Commission carrying out state regulation in the fields of electronic communications, radio frequency spectrum and postal services of Ukraine (of 07.09.2020 No.4066) .....	36
The draft law of Ukraine «On Amendments to Some Laws of Ukraine» (of 13.11.2020, No. 4378), submitted by the Cabinet of Ministers of Ukraine .....	37
The draft law on Amendments to the Criminal Procedure Code of Ukraine regarding the improvement of the effectiveness of the fight against cybercrime and the use of electronic evidence (of 01.09.2020 No. 4004), submitted by People's Deputy of Ukraine D.A. Monastyrskyi and others .....	38
The draft law on Amendments to the Criminal Procedure Code of Ukraine and the Code of Ukraine on Administrative Offences on enhancing the effectiveness of counteraction to cyberattacks (of 01.09.2020 No. 4003), submitted by People's Deputy of Ukraine D.A. Monastyrskyi and others .....	39
On Amendments to the Criminal Code and the Criminal Procedure Code of Ukraine (concerning the delimitation of jurisdiction over crimes committed in the sphere of use of information and telecommunications (automated) systems, telecommunications networks and facilities (of 17.07.2020 No. 3897), submitted by People's Deputy of Ukraine Fedienko A.P. and others .....	40

On Amendments to the Law of Ukraine «On the Security Service of Ukraine» on reforming the activities of the Security Service of Ukraine (24.03.2020 No. 3196-1), submitted by People’s Deputy of Ukraine Ustinova A.Y. and others. ....	41
On Amendments to the Law of Ukraine «On the Security Service of Ukraine» on reforming the Security Service of Ukraine (24.03.2020 No. 3196-D), submitted by People’s Deputy of Ukraine Zavitnevych A.N. and others.....	41
Draft Bylaws .....	43
Conclusions .....	44
<b>Gaps and Ambiguities in the Current Legislation.....</b>	<b>45</b>
<b>Roadmap for Reforming the Legal Framework for Cybersecurity .....</b>	<b>46</b>
<b>Annex A Legislation on Cybersecurity in Ukraine .....</b>	<b>49</b>
List of Ukrainian Laws.....	49
Bylaws on Cybersecurity in Ukraine .....	50
List of Draft laws and Draft Bylaws.....	52
The draft laws are registered in the Verkhovna Rada of Ukraine of the 9th convocation .....	52
Draft Bylaws .....	52
<b>Annex B Powers of Institutions Responsible for Cybersecurity.....</b>	<b>54</b>

## Preliminary Review

Preliminary Review<sup>1</sup> of cybersecurity legislation identified systemic gaps in regulation of cybersecurity and cyberdefense.



Ukraine made significant progress in developing cybersecurity components in current Ukrainian legislation; but two systemic tasks remain to be accomplished. The development, adoption and implementation of draft laws governing:

- Critical infrastructure in Ukraine
- Cybersecurity which the 2019 report refers to as «comprehensive».

Ukraine is at the initial stage of reconciling European Union (EU) legislation to its own legislation on cybersecurity and protecting critical infrastructure objects.

Ukraine laws and other regulations defining procedures of state regulation in the above areas, even without taking into account terms of their application, urgently need to be improved to update closer cooperation and interaction with the EU and NATO. In terms of introducing regulation of protection of critical infrastructure objects – development of a full-fledged basic law and establishing state policy regulating organizational, economic and financial measures is a priority.

Further, one of the primary factors that will contribute to strengthening common joint cyber space security between Ukraine and EU member countries will be harmonizing terminology systems, procedures and interaction protocols.

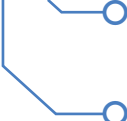
In 2019, IFES published its first Cybersecurity Legal Framework Overview. Since this publication, important draft legislations have been proposed to the Parliament. This updated overview assesses the Ukraine's progress in developing its cybersecurity legal framework and identifies gaps and components that require urgent attention from the legislator.



The first elements to be improved are:

- Current regulatory framework to address gaps and inconsistencies in line with international obligations, clear compliance with the Budapest Convention, Convention 108+, NIS Directive and other EU legislation;
- Developing and adopting a cybersecurity law and clarifying terminology and establishing incident reporting requirements for cybersecurity actors;
- Developing and improving legislation on public-private partnerships in cybersecurity and critical infrastructure protection;
- Adopting and implementing a law on critical infrastructure;
- Clarifying jurisdiction of cybersecurity and other legal subjects by amending the procedural and substantive norms of legislation;
- Clarifying legal provisions that define and establish characteristics of cybercrime which qualifies acts as crimes and clarifies criminal law on electronic evidence;

1 Legal basis of Ukrainian cybersecurity: general review and analysis. International Foundation for Electoral Systems in Ukraine, 2019 <https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf>

- 
- Differentiating jurisdiction and criminal responsibility for cybercrimes against state information resources, critical infrastructure and other objects; and,
  - Updating the Cybersecurity Strategy and developing a strategic cybersecurity plan for Ukraine.



## Introduction and Methodology

Ukraine has been developing a system of cybersecurity legislation for decades, but state legislation is usually a response to actions and events, external factors. Prevention legislation in our country has no established tradition, unlike in other countries.

Leaders in developing cyberdefense and cybersecurity systems are the United States and the United Kingdom. These countries have substantial budgets for development of the cyber component of their armed forces, as well as ongoing programs to ensure national security and protect critical infrastructure from cyberattacks.

Although Ukraine is actually in a state of hybrid warfare with Russia, this does not negate the need to direct efforts to study the experience of this neighboring country, if only to know and prepare for future cyber threats and predict and prepare a plan to address them.

This report provides an overview of the legal and regulatory framework for cybersecurity development in Ukraine based on international obligations and Ukraine's own strategic and policy documents.

In 2019, the first overview report « Ukrainian Cybersecurity Legal Framework: I Overview and Analysis», was prepared. This report is a continuation of the 2019 annual report. As a rule, the annual report contains review and analysis of documents adopted in the current year and materials on draft legal acts. Additionally, a review of the powers of the participants which are now responsible regulators and implementers of the documents, is administered.

International commitments were reviewed and clarified in view of the high-level setting of the course towards European integration and NATO. Materials on international commitments on data protection were included. New strategic documents were reviewed and perspectives for preparation of an updated Cybersecurity Strategy were provided.

Capabilities of participants in the cybersecurity ecosystem – the Ministry of Digital Transformation, the Information and Cybersecurity Council and working groups – were considered.

An extended review of the bylaws provides an opportunity to determine what needs to be regulated.

The gaps and ambiguities identified as a result of analysis in this report provide an opportunity to take another critical look at recently adopted documents and clarify certain regulations.

## Obligations Defined by International Agreements and Other Documents in the Field of Cybersecurity

Cybersecurity, as an important component of countering global threats, is gaining increasing support from governments in national security strategies; intergovernmental agreements; and, international instruments, conventions and United Nations model documents.

Critical vulnerabilities of countries' cyber space information infrastructure and the inability to solve the full range of problems that arise, necessitate unification of efforts, including building a collective cybersecurity system.

Last year, Ukraine decided on a pro-European course with a focus on joining NATO<sup>2</sup>. Ukraine enshrined these directions in the Constitution of Ukraine. Of all international commitments on cybersecurity, two have been identified as priorities for cooperation: A course towards European integration and accession to NATO.

An in-depth analysis of EU cybersecurity legislation suggests that EU institutions and policies do not consider cybersecurity measures separately from network and/or information system privacy measures; but, aim at harmonized action to protect the means, information and confidentiality as part of the cybersecurity and trust ecosystem.

The most important are the documents of the Council of Europe, to which Ukraine has been a member since 1995, specifically, the Convention on Cybercrime (the Budapest Convention); the Council of Europe's Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+).

They include EU documents on cybersecurity, which are primarily the NIS Directive<sup>3</sup>, Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on protecting natural persons with regard to processing personal data and free movement of data. Documents also include the repeal of Directive 95/46/EC (General Data Protection Regulation (GDPR))<sup>4</sup>, Regulation (EU) 2019/881 of the European Parliament and of the Council of April 17, 2019 on the European Union Agency for Cybersecurity and information and communications technology cybersecurity certification.

Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Regulation 881)<sup>5</sup> and Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on protecting personal data by competent authorities for prevention, investigation, detection and prosecution of criminal offenses

---

2 Law of Ukraine «On Amendments to the Constitution of Ukraine (on the strategic course of the state to gain full membership of Ukraine in the European Union and the North Atlantic Treaty Organization)» dated February 7, 2019 No. 2680-VIII <https://zakon.rada.gov.ua/laws/show/2680-19#n6>

3 Directive 2016/1148 of the European Parliament and of the Council dated 6 July 2016 on measures for a high common level of security of network and information systems throughout the Union [https://zakon.rada.gov.ua/rada/show/984\\_013-16#Text](https://zakon.rada.gov.ua/rada/show/984_013-16#Text)

4 Регламент (ЕС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про охорону фізичних осіб щодо обробки персональних даних та щодо вільного руху таких даних, а також скасування Директиви 95/46 / ЄС (Загальний регламент про захист даних): <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

5 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881>

is included in the document files. Execution of criminal sanctions on free movement of data and the repeal of Council Framework Decision 2008/977/JHA (Directive 680)<sup>6</sup> are part of the Council of Europe document files.

An important detail: The EU notes the need to combat cybercrime only if human rights are respected, this empowers the law enforcement system and safeguards rights.

Because of European integration obligations, international conventions of the Council of Europe, which are already part of Ukrainian legislation are the primary international legal standards of cybersecurity protection for our country. At the same time, EU acts in no way contradict the conventions; rather they reinforce them, although implementation of the EU acts will require norms with the national legislation. To date, Ukraine must pay more attention to implementation of the Council of Europe's conventions, which will be discussed.

## Budapest Convention and Convention 108+



The National Security and Defense Council (NSDC) at the conclusion of 2016 tasked the Ukrainian Government within three months to submit to draft laws to the Verkhovna Rada on implementation of the Convention on Cybercrime which provide the following:

- Giving law enforcement agencies authority to instruct owners of computer data (telecommunications operators and providers, other legal entities and individuals) on recording and storage of computer data required for detection of a crime for up to 90 days. Law enforcement would be authorized to extend this investigatory period to three years while normalizing instruction procedures;
- Establishing requirements for providing necessary information to telecommunications operators and providers at the request of law enforcement agencies to identify service providers and the route by which the information was transmitted;
- Introduction of blocking a court decision by telecommunications operators and providers of a certain information resource;
- Introduction of an effective mechanism for the use of electronic evidence in criminal proceedings, collected in the course of operational and investigative activities; and,
- Approval of protocols of joint actions by cybersecurity owners and managers of critical infrastructure information during detection, prevention, cyberattack cessation, cyber incidents and elimination of their consequences.

For more details on aspects of the implementation of this Decision of the NSDC, see the “Other Draft Laws” section of this study.

As for the implementation of Convention 108+, development of a national system of personal data protection continues. A new draft law on personal data protection is currently being drafted to implement the amendments to Convention 108, GDPR and Directive 680.

6 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities with a view to preventing, investigating, detecting or prosecuting criminal offenses or criminal penalties and free movement of such data and repealing Council Framework Decision 2008/977/JHA <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>

In September 2020, the Government adopted the Strategy for Combating Organized Crime and instructed the Ministry of Internal Affairs and interested central executive bodies to develop and submit to the Cabinet of Ministers a draft action plan to implement the Strategy within three months. At the conclusion of 2020, the draft plan is not publicly available.

Preventing and combating organized crime and criminal groups in high-risk areas should be administered by strengthening institutional capacity of law enforcement and other relevant government agencies. These bodies take adequate measures to respond to rapid development of financial and information technologies and deepen and expand ties at the national and international levels. Technology often facilitates communication of organized criminal groups.

The Strategy specifies functions for combating organized crime in an attempt to identify the subsystems of institutional support and determine a National Coordinator from among existing institutions. This task will require a detailed analysis and amendments to the current regulatory framework for law enforcement agencies. Given the number of institutions and laws, implementation involves high risks of non-compliance or delays.

Indeed, absence of a National Coordinator to fulfill international obligations negatively affects preparation for implementation of EU conventions and acts.

## EU Documents

In 2018, new EU rules came into force on establishing uniform requirements for electronic identification and providing electronic trust services, cross-border e-identification and cybersecurity, personal data protection. Some will be revised by the end of 2021 as the European Commission has already prepared draft amendments for discussion and adoption.

The need to bring principles of the digital sphere in Ukraine to the latest principles and standards of the EU is one of the most urgent tasks for the state and society. The first steps on this path have already been taken.

In August 2018, Ukraine developed and submitted to the EU a Strategy for Integration into the EU Digital Single Market together with an Action Plan to this Strategy, in accordance with Annex XVII of the Association Agreement between Ukraine, the European Union and the European Atomic Energy Community. The agreement was ratified by Law No. 1678-VII of 16.09.2014) (the Association Agreement between Ukraine and the EU)<sup>7</sup>.

The European Commission initiated a multi-phase process to assess implementation of Ukraine's existing obligations, administrative capacity and legislation.

According to the resolution Number 1106 on October 25, 2017 – “On the implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their member states, on the other hand”<sup>8</sup> – the administrative acts, which provided for development by executive authorities of the road map for implementation of the EU Directive provisions in the field of telecommunications are no longer valid.

---

7 Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other hand [https://zakon.rada.gov.ua/laws/show/984\\_011#Text](https://zakon.rada.gov.ua/laws/show/984_011#Text)

8 Resolution of the Cabinet of Ministers of Ukraine dated 25.10.2017 No. 1106 “On the implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other hand” <https://zakon.rada.gov.ua/laws/file/text/85/f473622n63.docx>

However, the vast majority of activities proposed in the draft roadmap were included in the Action Plan for implementation of the Agreement, approved by the above resolution, and correspond to the objectives set out in Annex XVII-3 to the Agreement, including implementation of the NIS Directive and Regulation (EU) 2016/679 (GDPR).

The NIS Directive is an integral part of EU cybersecurity legislation. The directive provides legal measures to increase the overall level of cybersecurity in the EU. It entered into force in August 2016. Under the transitional provisions of the document, member countries had 21 months to implement the Directive at the level of national law and more than six months to identify operators of basic services.

On June 27, 2019, Regulation 881 came into force through ENISA – the European Union Agency for Cyber Security – and on certification of cybersecurity in information and communication technologies.

The goal of EU cybersecurity acts is to strengthen ENISA's ability to help member countries overcome cybersecurity threats.

The Regulation 881 has two objectives:

- 1 Strengthening ENISA's role in supporting EU member countries in tackling cybersecurity threats and attacks, developing trust services and ensuring their safe use;
- 2 Establishing a pan-European cybersecurity certification system in which ENISA will play a key role.

According to Regulation 881, ENISA must coordinate preparation of proposed cybersecurity certification schemes and submit them to the European Commission for approval. The cybersecurity regulation will make it possible to issue European cybersecurity certificates and certificates of conformity for ICT products, services and processes in all EU member countries.

Regulation 881 provides tools through which businesses can verify that their products and services comply with EU cybersecurity standards. Certification is voluntary, unless otherwise provided by EU or member state acts (for example, on means of communication, receivers and routers). The European Commission should regularly review certification schemes for their mandatory nature.

A certification model can define one or more of the following levels of security: Basic, essential or high. At the basic level, ICT manufacturers or service providers will conduct their own compliance assessments. For essential or high levels of security, the assessment would be administered by national cybersecurity certification organizations.

EU member countries were scheduled to develop legislation to impose liability for breaches of Regulation 881.

Regulation 881 is part of EU's overall cybersecurity system which aims to increase security of the EU's digital environment and information services in the Digital Single Market.

On July 8, 2019, the 21st Ukraine-European Union Summit took place in Kyiv. The EU welcomed Ukraine's desire for further harmonization legislation with the EU in the digital economy; including cybersecurity, data protection and trust in the digital market. Ukraine and the EU expressed hope for further regular interaction, including a two-step assessment of Ukraine's regulatory adherence to the EU.

The European Commission is currently approving the draft Strategy for Ukraine's Integration into the EU Digital Single Market and agreeing on individual proposals. In August 2019, the EU mission to assess

harmonization of legal regulation in the Ukrainian digital market began its activities in Ukraine. The first meetings noted the high level of interest of all stakeholders to achieve concrete results and move to the next stage of bilateral dialogue and formation of a Joint Action Plan for Ukraine and the EU in the digital sphere.

The mission focuses on the telecommunications services sector, as unlike other sectors of the digital market, the Association Agreement contains clear commitments to implement several EU directives that directly or indirectly address cybersecurity of networks and systems (Directive 2002/58/EC amended)<sup>9</sup>.

Regarding implementation of the NIS Directive, communication with the EU continues, as this directive is not included in the annexes to the Association Agreement and the GDPR Regulation. The Government of Ukraine is currently taking measures to find solutions that will satisfy both parties to the Agreement.

The roadmap for implementing NIS Directive, GDPR and other documents related to network and information system security into Ukrainian legislation was planned within the mechanism established by the Association Agreement between Ukraine and the EU, including the action plan for the Association Agreement between Ukraine and the EU, the European Atomic Energy Community and their member countries<sup>10</sup>.

According to the Action Plan, implementation deadlines are in 2023.

Currently, a draft law has been registered in the Verkhovna Rada which would harmonize Ukrainian legislation with EU law, in particular, with the NIS Directive. Analysis of the draft law is provided in the section “Legislative level. Cybersecurity Law”.

---

9 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Confidentiality and Electronic Communications)  
<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>

10 Action plan for the implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other hand  
<https://zakon.rada.gov.ua/laws/file/text/85/f473622n63.docx>

## Conclusions



Ukraine is consistently moving toward its commitments, albeit with some obstacles and delays. Among the main obstacles are:

- Frequent changes of governments, which significantly slows down preparation of regulations at the level of draft laws and bylaws and increases time for approval of draft acts;
- Problematic issues related to law enforcement and judicial reform, which are manifested in the lack of institutional memory, lack of systematization in preparation of decisions and capacity to combat well-organized cybercrime;
- Draft laws amendments to the Criminal Code and the Code of Administrative Offenses must be submitted in separate drafts and they cannot be part of the final and transitional provisions of other draft laws which hinders the process of establishing new criminal offenses and liability for them;
- Miscommunication and disagreement between the government and telecommunications providers, which is reflected in the desire of operators and providers to minimize the obligation to ensure the security of communications at the stage of preparation of draft documents. From their point of view, this is justified, in particular, by the lack of need for state regulation of communications security, and, as a consequence, leads to the erosion of national security principles and interests of Ukrainian citizens.

A detailed review of proposed legislative amendments in this document in the context of institutional strengthening of cybersecurity provides for granting certain advantages to law enforcement at the expense of citizens' rights and freedoms which will further have a negative effect when international institutions assess rights and freedoms in Ukraine.

A positive signal is emergence of an understanding for close international cooperation in information and cybersecurity through the awareness that cyber space or information sovereignty cannot exist in understanding Ukrainian legislation.

According to the State Special Communications Administration, the definition by the EU of indicators of implementation of EU legislation into Ukrainian legislation also remains an issue. The problem is that definition of our specialists list of tasks to the plan of measures for integration is proposed from their professional position and knowledge and the lack of relevant official translations into the Ukrainian language. In some cases, there is a lack of appropriate authority associated with state bodies involved in European integration and no assessment of implementation of the proposed measure. Integration issues need to be improved in the future.

## National Legislation

The Constitution of Ukraine was amended in 2019 on the basis of «irreversibility of the European and Euro-Atlantic course of Ukraine», which required revision of certain legislation and harmonization of with other strategic documents. The Verkhovna Rada determined the principles of implementation for Ukraine's full membership in the EU and NATO.

The draft law on principles of state policy in European integration (reg. № 1206)<sup>11</sup>, was prepared in the Verkhovna Rada Committee on the Integration of Ukraine into the EU. But, prospects for its adoption are bleak. The Committee and the authors' group belongs to the opposition.

Another factor in the changes is the creation of the Ministry of Digital Transformation, which should coordinate all projects in digital transformation, cybersecurity and data protection. Its competence now includes:

- Participation in cryptographic and technical protection of information, cyberdefense, telecommunications by accessing the radio frequency resource of Ukraine. Protecting state information and requiring protection of information, telecommunications and information-telecommunication systems and facilities of information activities. In addition, utilizing state information to combat technical intelligence and the National System of Confidential Communications.
- Developing goals and objectives of state information policy and implementing intellectual property; establishing standards, norms, rules and procedures and determination of the functioning of executive bodies' official websites, state information-analytical systems, state information resources, electronic registers and databases. Adopting or amending regulations on personal data and intellectual property protection.

Another actor in the cybersecurity and data protection ecosystem is the Ministry of Digital Transformation. On the one hand, it may lead to a delay in fulfillment of obligations, since most acts on cybersecurity relate to the digital sphere of the state and require additional approval by the new body – although the Ministry is not responsible for formation and implementation of cybersecurity policy. On the other hand, it could help speed up the process, in case the Ministry of Digital Transformation takes over coordination between law enforcement agencies as an independent arbitrator. This responsibility is not related to security and defense.

Certain elements of the EU cybersecurity ecosystem still need to be created or improved in Ukraine.

According to the National Cybersecurity Index<sup>12</sup>, there is an absence of components of the cybersecurity system (see Table 1), although some items are not reflected correctly and will need clarification. Data is necessary for the National Cybersecurity Index.







---

11 The draft law on the Principles of State Policy in the Sphere of European Integration No. 1206 dated August 29, 2019 [https://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=66514](https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66514)

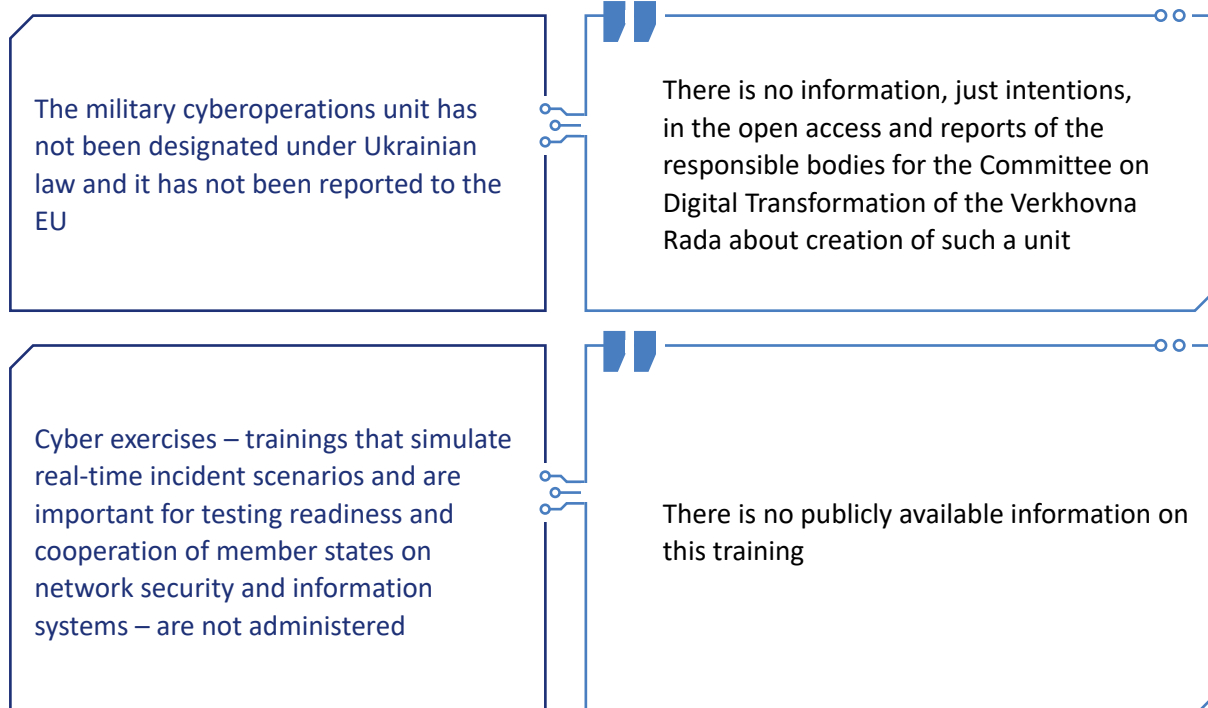
12 Національний індекс кібербезпеки <https://ncsi.ega.ee/ncsi-index/>



Table 1.

Missing Components of Cybersecurity According to the National Cybersecurity Index	Expert Comments
There is no cyberthreat analysis unit	 <p>This unit may exist in one of the Ukrainian intelligence services; but, no information about it is publicly available</p>
Annual public reports are not made publicly available	 <p>Public reports are not currently required by law</p>
There are no requirements for cybersecurity competencies for primary and secondary school students	 <p>Requirements for cybersecurity competencies for primary and secondary school students and older citizens need to be developed</p>
There are no regional or international cybersecurity organizations in Ukraine	 <p>This point primarily concerns EU countries; but there are no such organizations in Ukraine</p>
In the last three years, at least one capacity building project for another country is not funded or there is no overall organization	 <p>Ukraine's participation in such projects is possible, but as a priority at the state level such a measure is not planned</p>
There is no standard for cybersecurity for the public sector	 <p>Resolution of the Cabinet of Ministers of March 29, 2006, Number 373, approved the Rules for Ensuring Information Protection in Information, Telecommunication and Information-Telecommunication Systems pursuant to Article 10 of the Law of Ukraine "On Information Protection in Information and Telecommunication Systems" for the public sector. But, indeed, both of the regulations mentioned here need significant revision.</p>

<p>There is no competent governmental body in the field of cyber or information security with the authority to monitor public and private digital service providers for compliance with cyber or information security requirements</p>	<p>At the level of legislation there is no term, “digital service providers”</p>
<p>There is no regular monitoring of cybersecurity measures</p>	<p>It is possible to organize monitoring only with the use of the control function of the Verkhovna Rada due to lack of cyber security agency</p>
<p>There is no regulation of the time stamp in electronic trust services</p>	<p>Article 26 of the Law of Ukraine “On Electronic Trust Services” and the Resolution of the Cabinet of Ministers of Ukraine of November 7, 2018, Number 992, regulated this issue at the time of compiling the index and it will be necessary to clarify which body provided information to index compilers.</p>
<p>The Government has not designated a single point of contact for international cybersecurity coordination</p>	<p>CERT-UA, the government computer emergency response team of Ukraine, which operates within the State Center for Cyberdefense of the State Special Communications Administration since 2009 is an accredited member of the Forum of Security Incident Response Teams <a href="#">FIRST</a></p>
<p>There is no cyber crisis management</p>	<p>Indeed, changes in legislation is required and the development of institutional capacity</p>



## National Security Strategy

President Volodymyr Zelensky approved the new National Security Strategy of Ukraine – the NS Strategy – on September 14, 2020.

Ukraine's national interests and security include strengthening the national cybersecurity system to effectively combat cyberthreats in today's security environment.



Current and projected threats to national security and interests of Ukraine are identified, taking into account foreign policy and domestic conditions:

- Globalization causes the spread of international terrorism and international crime in cyber space;
- International competition is intensifying and the use of instruments of influence is expanding,
- Russia continues its hybrid war and uses political, economic, informational, psychological, cyber and military weapons;
- The following factors do not contribute to protection of critical infrastructure: Deterioration of its technical condition, underinvestment in renovation and development, unauthorized interference in the operation of critical infrastructure, ongoing hostilities, and the temporary occupation of Ukraine.



The NS Strategy defines foreign and domestic political activity to ensure national interests and cybersecurity:

- Active participation of Ukraine in counteracting cyberthreats;
- military security is developing capacity to deter and strengthen the combat capability of the Armed Forces, a prepared and motivated military reserve and effective territorial defense;
- Protection against non-military threats from Russia and other countries to state sovereignty, territorial integrity, democratic constitutional order and other vital national interests;
- Active and effective counteraction to intelligence and subversive activities, special information operations and cyberattacks. Russian and other subversive propaganda is a priority for law enforcement and special intelligence.



Ukraine will introduce a national system of resilience to ensure a high level of readiness of society and the state to respond to a wide range of threats, which will include:

- Risk assessment, timely identification of threats and vulnerabilities;
- Effective strategic planning and crisis management, including implementation of universal crisis response protocols and recovery in line with NATO recommendations;
- Effective coordination and clear interaction of security and defense sector organizations, territorial communities, business, civil society and the public in preventing and responding to threats and coping with emergencies;
- Distributing knowledge and skills; and,
- Establishing and maintaining reliable channels of communication between government agencies and the population throughout Ukraine.

The NS Strategy identifies the need to create an effective system of security and resilience of critical infrastructure, based on a clear division of responsibilities between and public-private partnerships.

The primary task of cybersecurity system development is to guarantee cyber resilience and cybersecurity of national information infrastructure in conditions of digital transformation.

To systematically protect Ukraine from threats to national security, it is necessary to develop the security and defense sector by creating a national cybersecurity system, build modern capabilities of cybersecurity and cyberdefense and strengthen their coordination system.

## Cybersecurity Strategy

According to Paragraph 2 of Article 31 of the Law of Ukraine “On National Security of Ukraine”<sup>13</sup> the preparation of the Cybersecurity Strategy of Ukraine is organized on behalf of the President of Ukraine by the National Coordination Center for Cybersecurity (NCCC) after approval of the overall National Security Strategy of Ukraine.

On September 14, 2020 President Zelensky, by Decree Number 392, enacted the decision of the National Security Council titled, “On the National Security Strategy of Ukraine”, where Paragraph 3 gave instructions to the Cabinet of Ministers and state agencies in the national security to submit within six

months to the National Security and Defense Council a draft Strategies of Information Security and Cybersecurity Strategy.

“After the President approved the NS Strategy of Ukraine, a Working Group was formed on the basis of the NCCC to develop the Cybersecurity Strategy. Representatives of key state cybersecurity agencies began to submit their proposals to the NCCC,”<sup>14</sup>, the National Security Defense Council press office said in a statement, which is now missing from the website but remains in numerous media reports.



The Law of Ukraine «On Basic Principles of Cybersecurity in Ukraine»<sup>15</sup>, or the (Law on Cyber Security:

- Ensures formation and implementation of state policy in cybersecurity, the national interests of Ukraine in cyber space and the fight against cybercrime;
- Establishes the legal basis for organization and provision of necessary forces and resources of the national cybersecurity system;
- Ensures the information security audit system at critical infrastructure, except for critical infrastructure objects in the banking system of Ukraine;
- Defines NCCC obligations to submit proposals to the President on formation and refinement of the Cybersecurity Strategy of Ukraine.

The Government of Ukraine should create an interdepartmental Working Group to draft a Cybersecurity Strategy and an Information Security Strategy and resolve conflicting powers defined for the NCCC and the Government. Now there is no information about the existence of an order in public sources. The deadline for preparation of the Cybersecurity Strategy is March 14, 2021.

In December 2020, a memorandum between the Office of the National Security and Defense Council, the Ministry of Digital Transformation and the Administration of the State Service of Special Communications and Information Protection on Interaction and Cooperation in the Field of Information and Cybersecurity was adopted which aims to improve mechanisms to enhance capabilities of the national cybersecurity system. The parties shall establish an Information and Cybersecurity Council – the Council – as a body of expert support for the parties’ activities in determining:

- Gradual decentralization of the model of management of the national cybersecurity system on the principles of self and co-regulation;
- Improvement of legal and regulatory support for developing cybersecurity and cyberdefense;
- Implementation of international standards, risk-oriented approaches and recognized good practices in cybersecurity and information security and gradual change of outdated standards in technical protection of information;
- Creating a national terminology that complies with European norms and standards in cyberprotection, information security and cybersecurity;

13 Law of Ukraine “On National Security of Ukraine” No. 2469-VIII dated June 21, 2018 <https://zakon.rada.gov.ua/rada/show/2469-19#Text>

14 Specialists of the National Coordination Center for Cybersecurity under the NSDC started to develop a Cybersecurity Strategy of Ukraine, Ukrinform, <https://www.ukrinform.ua/rubric-polytics/3105556-u-rnbo-pocali-rozroblati-strategiu-kiberbezpeki-ukraini.html>

15 Law of Ukraine «On the Basic Principles of Cybersecurity of Ukraine» dated October 5, 2017 No.163-VIII <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

- 💬 Solving decriminalization of ethical hacking and penetration testing;
- 💬 Implementation of organizational and technical models of cyberdefense;
- 💬 Building trusting relationships between cybersecurity actors when implementing measures to protect critical infrastructure from cyberthreats;
- 💬 Tools for practical implementation of public-private partnerships;
- 💬 Deploy a system to detect and respond to cyber incidents and cyberattacks and eliminate their consequences;
- 💬 Deploy an information exchange on real and potential cyberthreats;
- 💬 Submit proposals to national strategic documents related to development of national cybersecurity;
- 💬 Develop a methodology for conducting a cybersecurity survey of Ukraine;
- 💬 Provide recommendations on how to implement international standards for technical protection of information, including ISA/IEC 62443, for automated process control systems of critical infrastructure;
- 💬 Provide proposals for liberalizing the cybersecurity services market;
- 💬 Assess current and potential cyberthreats in Ukraine;
- 💬 Public oversight over implementing the Cybersecurity Strategy of Ukraine and evaluating effectiveness;
- 💬 Providing recommendations on developing regulations for the exchange of information about cyber incidents, both at the national level and within individual industries;
- 💬 Evaluating effectiveness and areas of improvement of the training system for cybersecurity professionals;
- 💬 Developing cyber hygiene in Ukraine and improve cyber literacy through development of nationwide programs to disseminate cybersecurity knowledge;
- 💬 Developing new projects that will contribute to development of cybersecurity in Ukraine;
- 💬 Create a national network of CSIRT, SOC and CERT;
- 💬 Implement European legislation in the practice of the national cybersecurity system of Ukraine;
- 💬 Process mechanisms for effective auditing of critical infrastructure in implementation of measures to protect against cyberthreats;
- 💬 Organize “Bug Bounty” programs for important state information resources, as well as critical information infrastructure;
- 💬 Prepare recommendations to improve the state of cybersecurity of critical infrastructure;

- 💬 Promote educational activities for all national cybersecurity actors to improve their cybersecurity and cyberdefense awareness;
- 💬 Develop mechanisms for conducting and organizing cybertrainings;
- 💬 Form a network of key public events on cybersecurity, including conferences, exhibitions, and academic events, that will be fully supported by all cybersecurity actors as major confidence-building platforms.

Potentially, this structural element of Ukraine's cybersecurity ecosystem will contribute to its development. But so far, questions remain open as to exactly which government department will create this consultative and advisory body; its status; how support for decisions will be organized; and, how the Council's work will be organized.

According to business and public stakeholders, the procedure for electing members of the Board should be improved in the future – a clearer criteria for experts should be put forward and the composition of the organizing committee for the selection of Board members should be announced. The Council statute is still under discussion.

The list of tasks and hopes that participants in the memorandum have for this body is too optimistic, given the entirely volunteer basis of its activities and the experience of existing Working Groups under the Verkhovna Rada Committee on Digital Transformation and under the National Security and Defense Council on the Cybersecurity Strategy development.

### **Legislative Level: The Cybersecurity Law**

Cybersecurity legislation in Ukraine includes documents listed in Annex A, the "Legislative Framework for Cybersecurity in Ukraine".

The Verkhovna Rada Committee on Digital Transformation – the Committee – as part of its oversight function under the Cybersecurity Law, conducted a series of events: Hearings and meetings of the Committee covering "National Cybersecurity and Cyberdefense of Ukraine, Including Critical Infrastructure" and hearings on "Implementation of the Roadmap for Ukraine's Integration into the EU Single Digital Market".

On December 23, 2020, the Committee held a hearing on "National Cybersecurity and Cyberdefense of Ukraine, including Critical Infrastructure"<sup>16</sup>.

Following the hearings and in view of the constant criticism from the expert community of the Cybersecurity Law, the Committee organized an evaluation and analysis of this Law by an independent expert. Results of the analysis, according to the PLS methodology, are posted on the Committee's website.

Another reason for choosing to evaluate this legal act is the control function of the Verkhovna Rada and the Committee directly defined in the Law on Cyber Security, specifically the Verkhovna Rada monitors compliance with the law implementing cybersecurity measures consistent with the Constitution.

<sup>16</sup> On December 23, the Committee on Digital Transformation held a hearing on «National Cybersecurity and Cyberdefense of Ukraine, including critical infrastructure» [http://komit.rada.gov.ua/news/main\\_news/povidomlen/73496.html](http://komit.rada.gov.ua/news/main_news/povidomlen/73496.html)

The evaluation is in line with previous IFES recommendations, published in 2019, on the need to prepare a new draft law and repeal the framework Law of Ukraine “On the basic principles of cybersecurity in Ukraine”.

On February 19, 2020, the Committee considered compliance with Part Three of Article 15 of the Cybersecurity Law on an independent audit of the main national cybersecurity actors and effectiveness of cybersecurity systems of the state. It was determined that the national cybersecurity actors have not fulfilled the requirements of Part Three of Article 15 of the Cybersecurity Law.

As a result of consideration of reports on national cybersecurity, the Committee raised the issue of “Cybersecurity, critical infrastructure, electronic communications in Ukraine: state, problems, solutions”, which were scheduled for April 15, 2020, but postponed tentatively to 2021 because of the coronavirus lockdown.

The point of view of national cybersecurity actors is uniform; all expressed the same positions regarding non-compliance with the Law to organize and conduct an audit:

- 1 The public authorities, activities of which are provided by the military on the rights of subordination (the National Bank of Ukraine is an exception). These circumstances make it necessary for the auditor to have special access to information;
- 2 The inability to implement the law;
- 3 Strict restrictions on the ability to select international audit firms.

Today, the Verkhovna Rada Committee on Digital Transformation, responsible for cybersecurity, deploys a Working Group «On the formation of conditions, creation and management of information cybertechnologies and the formation of national legislation in the field of cybersecurity of Ukraine» at a sufficiently expert and professional level to prepare proposals for improving legislation in regulating cybersecurity and protection of critical infrastructure.

The Working Group included representatives of national cybersecurity, representatives of cybersecurity from business organizations, cybersecurity experts and representatives of public associations.

The Working Group is currently working on the implementation of the NIS Directive and directives of the United Nations and other international organizations. Information on the draft law on critical infrastructure is more detailed in the section below.

Activity in the direction of improving cybersecurity legislation is related to conclusions of the analysis of cybersecurity legislation contained in numerous expert reports of various institutions and organizations (EU, IFES, MITER and the UNDP).



Particular attention is paid to the growing role of public-private partnerships:

- Preparing proposals for development of strategic documents in cybersecurity;
- Developing national and international standards;
- Implementing the advisory function;
- Expanding the range of participants in scientific and technical cooperation and use of scientific achievements by the state, cooperation and collaboration of science, business and production;
- Conducting broad consultations with stakeholders within advisory bodies.



Eight draft laws have been registered in the Eighth Parliament to regulate cybersecurity (see Annex A), which:

- 1 Establish a legal basis for activities in electronic communications and the radio frequency spectrum;
- 2 Regulate legal relations on data processing and protection when using cloud computing technology and providing cloud services.
- 3 Define the legal status of the National Commission, which regulates electronic communications, radio frequency spectra and postal services of Ukraine.
- 4 Regulate the functioning and protection of critical infrastructure as part of Ukraine's national security legislation. Introduce a regulator which will be the National Commission for Critical Infrastructure Protection of a central executive authority with special status.



As of 2019, pending and unresolved issues were:

- Jurisdiction over investigation of crimes committed in computers, systems, computer networks and telecommunications networks, state information resources and CI objects;
- Establishing and strengthening liability for cyberterrorism and cybercrime;
- Strengthening accountability for violations of legislation in combating cybercrime and information security;
- Countering threats to information security in national security and defense.



Given the need to address a significant volume of issues in various areas, the Working Group proposed to develop several draft laws:

- On cybersecurity. The future draft law proposed for consideration is being discussed in the Working Group;
- On critical infrastructure;
- On amendments to the Criminal and Criminal Procedure Codes of Ukraine regarding implementation of the Convention on Cybercrime regarding electronic evidence;
- On the cybersecurity regulator;
- On information security.

The legislation must establish content, timing and conditions of a crisis, mechanisms for dealing with crises in cyber space, crisis response measures for cyberthreats and response.

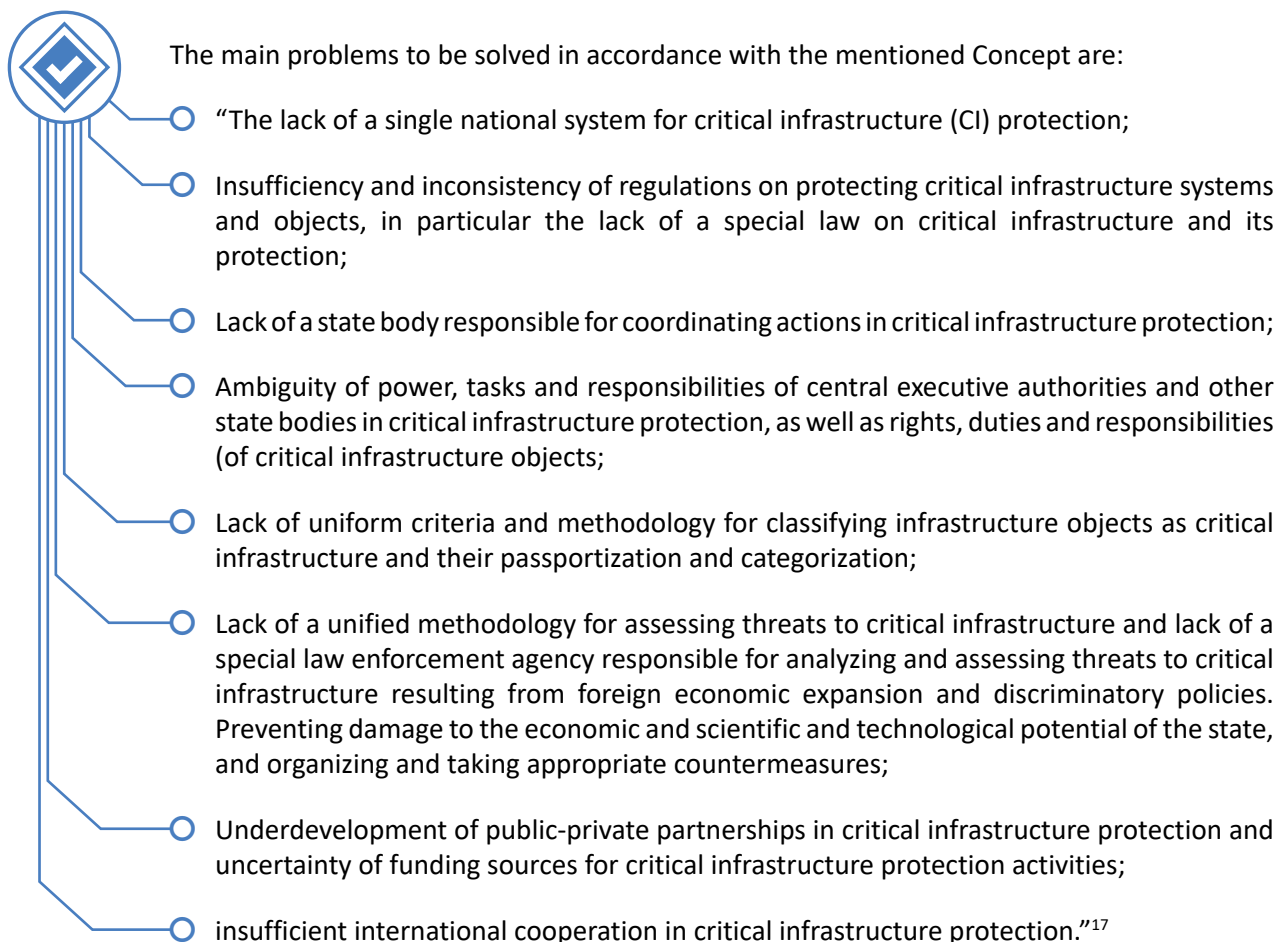
The legal basis for information technology in public administration is legislation on informatization, information protection in ITS and e-government.

The list of laws to be amended has not yet been compiled. Harmonization of terminology in terms of cybersecurity of Ukraine, the EU and NATO will require amendments to other existing laws in Ukraine, which define basic terminology – data, information, personal data and informatization.

At the legislative level, there have been no significant changes since the last report—proposals for legislative amendments remain in preparation for consideration by the Rada and will be described in more detail in this report in the sections on draft laws.

## Level of Bylaws

At the level of bylaws, there have been shifts toward organizing the process of protecting critical infrastructure objects, or CIO. Creation of the state system for protecting critical infrastructure objects was approved in 2017 by the order of the Cabinet of Ministers of Ukraine Number 1009 of December 6, 2017.



According to the Cybersecurity Law, a dozen acts of the Cabinet of Ministers were scheduled to be developed. This past year – 2020 – was fruitful for preparation and adoption of acts of the Cabinet of Ministers which had been prepared since the Cybersecurity Law went into effect in 2018. However, there has not been coordination with the authorities. Particularly unfavorable was frequent change of government during this period, procedurally requiring new drafts with each new prime minister. Some are in draft form due to inconsistencies and require revision and approval.

The central executive authority that ensures formation of and implements state policy in special communications, information protection, cyberdefense of telecommunications and use of radio frequency resources of Ukraine is the State Service of Special Communications and Information Protection of Ukraine, or SSSCIP. This organization has with special status and are directed and coordinated by the Cabinet of Ministers through the Deputy Prime Minister and Minister of Digital Transformation.

The special status of this body is that it is both an executive authority and part of the security and defense sector of Ukraine. It is this fact that is an obstacle to perform functions of the cybersecurity sector regulator. Although the Regulation on SSSCIP in October was amended to go into effect on January 1, 2022 to administer state market surveillance within one of its areas of responsibility, this function can only be realized by the cybersecurity regulator.

It should be noted that the SSSCIP during 2020 conducted «homework» with the draft laws, which were developed earlier, which significantly improved their content and clarified the regulation. However, the SSSCIP tried to control related systems, such as compliance assessment and audit, and noted the National Anti-Corruption Bureau of Ukraine, or NABU, in its conclusions. See more in the Draft Bylaws section.



Important issues have been resolved at the level of bylaws regarding critical infrastructure facilities:

- Procedure for classifying facilities as critical infrastructure objects;
- List of sectors and sub-sectors and their services to state infrastructure;
- Methodology for categorizing critical infrastructure objects;
- Procedure for compiling the list of critical information infrastructure objects;
- Procedure for entering critical information infrastructure objects into the state register of critical information infrastructure objects and ensuring its functioning;
- Criteria, methodology and mechanisms for determining objects of critical infrastructure in the banking system; and,
- Organizational framework for conducting cybersecurity surveys of critical information infrastructure, state information resources and information whose protection is required by law.

The gap in these documents is the lack of implementation deadlines which will require preparation of a separate document of the Cabinet of Ministers.



Critical infrastructure includes banks, the stable functioning of which ensures stability of the banking system and is essential to the economy and state security. The National Bank of Ukraine, or NBU, and banks which meet at least one of the following criteria:

- Included in the list of systemically important banks;
- Included in the list of banks authorized to operate during a special period; and,
- The state directly or indirectly owns more than 75 percent of its authorized capital.

The question remains open about definition of other critical infrastructure objects in the financial sector as regulated by the NVU. The Cybersecurity Law authorizes the NBU only to define critical infrastructure in the banking system.

17 On approval of the Concept of creation of the state system of protecting critical infrastructure, Order of the Cabinet of Ministers of Ukraine No. 1009 of December 6, 2017 <https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80>

In December, the Concept of Development of Artificial Intelligence was approved, one of the tasks and results of which is structural implementation of artificial intelligence technologies in the national cybersecurity system and strengthening capabilities of its actors. The drawback of the Concept is its authors do not consider artificial intelligence as a threat to cybersecurity. Most of the leading countries in the world in their updated cybersecurity strategies have identified new types of threats – digitalization and artificial intelligence. In Ukraine, only benefits from introduction of artificial intelligence is recognized, which is doubtful, given the unexplored nature of this issue.

Vulnerability detection and response to cyber incidents and cyberattacks, approved by the Cabinet of Ministers on December 23, 2020 through Number 1295, identified the State Center for Cyberdefense of SSSCIP as responsible for vulnerability detection and response to cyber incidents and cyberattacks.

Components of a vulnerability detection and response system for cyber incidents and cyberattacks are a:

- 1 Subsystem of the Ukrainian government's Computer Emergency Response Team, or CERT-UA, which provides centralized collection and accumulation of information on cyberthreats and cyber incidents from various sources, including open sources;
- 2 Subsystem for detecting and responding to cyberattacks at the workstation and server level ("endpoints"), which provides detection of malicious activity, responding with actions to eliminate, minimize, isolate and block processes used by malware;
- 3 Subsystem for collecting telemetry of information and telecommunication systems, or active sensors.

Installing sensors on state-owned cybersecurity objects and their installation for the non-state sector upon a separate application of an owner of such an object to the State Center for Cyberdefense of SSSCIP was also determined to be a priority.

Parameters of telemetry information transmitted from other state and non-state systems of cyberdefense objects to systems of vulnerability detection and response to cyber incidents and cyberattacks, interaction between security administrators of the systems of vulnerability detection and response to cyber incidents and cyberattacks and security administrators of the cyberdefense object must be coordinated by the cyberdefense object owner with the State Center for Cyberdefense of the SSSCIP.

The SSSCIP should determine the procedure for transferring sensors.

Information sharing and its protection in the system of vulnerability detection and response to cyber incidents and cyberattacks should be administered in accordance with the law; but, so far it is impossible to assess effectiveness due to lack of information about the actual law. Unfortunately, this act has not been publicly discussed and it is impossible to determine whether it will fully regulate the process of interaction in the detection of vulnerabilities and information sharing.

On December 23, 2020, the Government approved the order of the pilot project which introduces a number of organizational and technical measures to identify vulnerabilities and shortcomings in the software of public information resources, according to the Ministry of Digital Transformation<sup>18</sup>. An automated remote scanning of these resources will be introduced, which will assess the state of their security and promptly identify and eliminate deficiencies and vulnerabilities.

Three nationwide election campaigns took place in Ukraine in 2019 and 2020. As the Central Election Commission noted in the CEC's Strategic Plan for 2020-2025, "the 2019 election campaigns revealed a number of external threats that could negatively affect elections in Ukraine. These include the spread of misinformation through the Internet, in particular in social networks, interference in the elections of foreign states, cyberattacks on the information systems of the Commission..."<sup>19</sup> Planned defense against cyberthreats include:

- 1 Upgrading the redundancy system of information systems and services and increasing employee awareness of cyberthreats and their ability to adequately counter them;
- 2 Introduction of regular technical and security audits of the CEC's systems and the State Voter Register Administrator Service.

The need to develop and adopt a comprehensive cybersecurity strategy and to conduct regular post-election audits to assess the effectiveness of the cybersecurity system was also noted.

The State Regional Development Strategy for 2021-2027 asserts objectives for development of security infrastructure, including building the National Resilience System at the regional level, implementing new approaches in the protection of critical infrastructure and creating conditions for development of cybersecurity infrastructure and cyberdefense.

## Conclusions

Given the changes that have taken place in regulation at the level of bylaws, during the second half of 2021 and early 2022, it will be necessary to analyze effectiveness of their implementation. It would be desirable to introduce a mechanism for continuous monitoring at the level of strategic documents – a Cybersecurity Strategy and Information Security Strategy.

Given the need to implement EU legislation and harmonize different approaches to cybersecurity, when updating the cybersecurity strategy, a separate section on network and information security and the milestones, goals and performance indicators proposed by ENISA should be envisaged. Or alternatively, the ENISA recommendations can be implemented in two strategies – cybersecurity and network and information security. The cybersecurity strategy is part of strategic planning for national security and defense while the strategy for network and information security will address all other industries segments of society.

An important direction seems to be defining and fixing the difference between information security and cybersecurity given the President's instruction to develop two separate strategies.

It is recommended to pay special attention to recording in the Cybersecurity Strategy, a mechanism for periodic review of challenges and threats, which should be the basis for development of the Strategy measures.

18 The Ministry of digital transformation and the State Special Communications Service initiate the implementation of a cyber incident monitoring system Press Office of the State Special Communications Service: <https://thedigital.gov.ua/news/mintsifra-ta-derzhspetsvnyazku-initsiyue-vprovadzhennya-sistemi-monitoringu-kiberintsidentiv>

19 On the Strategic Plan of the Central Election Commission for 2020-2025. Resolution, Plan dated 11.06.2020 № 102: <https://zakon.rada.gov.ua/laws/show/v0102359-20#Text>

Ukraine's Cybersecurity Strategy should establish basic principles for planning, budgeting, implementation and analysis of the effectiveness of measures for its fulfillment. They should not contradict the measures and principles defined by legislation. It is necessary to formulate mechanisms for preparation and evaluation of implementing the Cybersecurity Strategy on the basis of ENISA recommendations for future periods and provide the possibility to revise the strategy taking into account possible threats and challenges during its operation.

The most necessary measures to be reflected are to provide cybersecurity actors and critical infrastructure objects with the necessary human, information and analytical, financial and technical resources to implement the Strategy.

Regulatory impact analysis and evaluation of cybersecurity strategy effectiveness should be integral steps in preparation of strategic documents. Particular attention should be paid to proper financial support for preparing strategic documents.

Currently, no central executive authority in Ukraine is empowered to coordinate cybersecurity activities in areas other than security and defense. This function is entrusted to the National Security and Defense Council, the coordinating body for national security and defense under the President, according to Article 107 of the Constitution of Ukraine.

It is necessary to develop a new model for a national cybersecurity system and cybersecurity agencies with clearly distributed authority and a protocol for interaction between system components in the executive branch and the security and defense sector.

There seems to be an urgent need to develop a nationwide target program on cybersecurity to organize development of missing or insufficiently provided components of the cybersecurity ecosystem. The State Targeted Program for Development of Special Communications, Information Protection and Counteraction to Technical Intelligence for 2016-2021 (it is classified) is now in place. It partially contains scientific research, development of modern special communications, information protection, cyberdefense and counteraction to technical intelligence.

## Draft Laws








### The Draft Law on Critical Infrastructure – New Version









The draft law “On Critical Infrastructure” was prepared by the Working Group.

It is proposed to regulate protection of critical infrastructure. This draft law should become an integral part of Ukrainian legislation in the field of national security. The draft law is being prepared for registration.

Separately, it should be noted that the new 2021 draft law, compared with the older draft law, was changed in the structure and approaches to formation and implementation of regulatory authority in the protection of critical infrastructure objects and conducting an independent audit of participants.

The 2021 draft law proposes:

-  Define the concepts of «security of critical infrastructure», «vital functions», «protection of critical infrastructure», «category of critical infrastructure object», «crisis situation», «critical infrastructure», «critical technological information», «critical infrastructure operator», «national critical infrastructure protection system», «unauthorized interference», «protection of critical infrastructure», «security passport», «infrastructure object criticality level», «regime of critical infrastructure operation», «critical infrastructure object register», «critical infrastructure sector», «critical infrastructure resilience» and «sector body in the field of critical infrastructure protection»;
-  Define basic principles of operation of the national CI defense system and levels of management of the national CI defense system;
-  Formulate criteria for classifying facilities as CI. Classifying facilities to critical infrastructure is administered on the basis of criteria that determine their social, political, economic and environmental importance to ensure national defense, state security and law and order. Their importance for implementation of vital functions and vital services indicates the existence of threats, the possibility of crisis situations due to unauthorized interference with their functioning, function disruptions, human factor or natural disasters and the duration of work to eliminate consequences until full restoration of the normal regime;
-  Identify vital functions, the violation of which leads to negative consequences for the national security of Ukraine;
-  Coordinate actions of the national critical infrastructure protection system to form and introduce a register of critical infrastructure objects;
-  Oblige operators of critical infrastructure objects to prepare and submit for approval to sectoral authorities in critical infrastructure protection, and to the entity entrusted with physical security and a security passport for each critical infrastructure object;
-  Introduce a regulator which should be the National Commission for Critical Infrastructure Protection – a central body of executive power with special status. Activity of the body will be directed, coordinated and controlled by the Cabinet of Ministers. Transitional provisions of the draft law also require the Cabinet of Ministers to establish the National Commission for Critical Infrastructure Protection and ensure a competition for selection of the Chairman and members of the National Commission for Critical Infrastructure Protection, as proscribed by the Law of Ukraine “On Public Service” before enactment of the CI law;

-  Select the model, form and implementation by the regulator in critical infrastructure protection based on formation and implementation of public policy, functional management of the national system and coordination. Analysis of the future body confirmed the need to create a central body of executive power with special status;
-  Define the authority of sectoral and functional authorities and operators of critical infrastructure objects;
-  Amend Ukraine to form a legal basis for introduction of a comprehensive legal institution and determine powers of sector regulators in this area. Changes were made to the Civil Protection Code; and, the laws «On the Basic Principles of Cybersecurity of Ukraine», «On Information», «On Operational-Search Activity», «On Counterintelligence Activity», «On the Legal Regime of Emergency Situation», «On the Legal Regime of Martial Law», «On the Cabinet of Ministers of Ukraine», «On Security Activity», «On Defense», «On the Armed Forces of Ukraine», «On the National Bank of Ukraine», «On the National Police», «On the National Guard of Ukraine», «On the Security Service of Ukraine», «On State Service of Special Communication and Information Protection of Ukraine», «On Local Self-Government in Ukraine», «On Protection of Information in Information and Telecommunication Systems», «On Local State Administrations», «On Insurance» and «On Banks and Banking Activity”;
-  Consider problems that may arise with critical infrastructure objects (CIO) , to resolve interaction of the national system of protection of critical infrastructure with other protection systems in national security – with the unified state system of prevention, response and termination of terrorist acts and minimization of their consequences; with the national system of protection of resources in information and telecommunication systems; with the national system of cybersecurity; with law enforcement agencies in counteracting crime; and, with the unified state system of civil protection;
-  Introduce parliamentary and public control in critical infrastructure protection;
-  Introduce an independent external assessment of the activities of the Authorized Body which is administered by conducting an annual external audit of its activities. Independent external assessment of the activities of the critical infrastructure protection system is carried out once every three years. External audit of activities of the Authorized Body shall be conducted by Ukraine’s Accounting Chamber;
-  Introduce application of administrative and economic sanctions to central and local executive authorities such as civil-military administrations, local governments, territorial communities and their officials and officers, operators of critical infrastructure objects, in case of violations of legislation protecting critical infrastructure. Application of this provision will be postponed for three years due to the need to study practice of application of the law, formation of legal consciousness of owners and operators of CIO and detailing these types of liability;
-  Establish voluntary and compulsory insurance to cover financial losses caused by a crisis situation in accordance with the Law of Ukraine «On Insurance». The list of critical infrastructure objects, insurance risks for which mandatory state insurance applies in a crisis situation, shall be approved by the Cabinet of Ministers.

In the final provisions of the legislation, defining the procedure for it becoming law, an exception to the general procedure is made. In three years from the date of entry into force of this law, the provisions on mandatory insurance of critical infrastructure objects will be operational and enforced.



These provisions are postponed to develop a practice of applying this law, achieving adequate experience and awareness and the ability to plan for the financial costs of the stakeholders.

### **The Draft Law on Cloud Services (Dated June 16, 2020 – Number 2655)**

The draft law on Cloud Services (Number 2655) was submitted by Members of Parliament Fedienko A.P., Kriachko M.V., Sokha R.V. and Chernev E.V. on April 28, 2020. The Verkhovna Rada website does not have the text of the draft prepared for second reading.





The draft law's primary purpose is to regulate legal relations associated with the processing and protection of data using cloud computing technology and provision of cloud services.

The draft law lays the foundation for development of platforms of information and communication technologies based on cloud computing and implementation of the policy of cloud first priority in public administration, education, science and public life and which could be the impetus for more effective interaction between the state and society.




According to the authors of the draft law, the use of cloud computing systems will reduce the cost of building and expanding computing facilities, including for information as protected by law. Only secret information that cannot be placed outside the controlled area of the information owner would require separate processing procedures.


The draft law also provides for amendments to the law «On Protection of Information in Information and Telecommunication Systems», «On Protection of Personal Data» and «On Public Procurement» to regulate processing certain types of information in cloud computing systems and cloud services procurement by public authorities, local authorities and military units. The draft law would be established in accordance with the laws of state enterprises, institutions and authority who have been delegated such power.

The legislation proposes to:

-  Define the concept of «cloud computing», «cloud services», «cloud service provider», «cloud service user», «cloud resources», and «data processing center»);
-  Introduce definitions and a list of cloud services and how they fit into methods of Ukrainian legislation to establish requirements for the cloud service provider for public customers;
-  Establish the legal framework for cloud services and define essential terms of the cloud services contract; and,
-  Determine specifics in providing and consuming cloud services by national and local government authorities with an emphasis on personal data and information security in cloud services.

Some disadvantages of the draft law should also be noted:

-  Security of the cloud computing system and responsibility for violations are not regulated in detail;
-  Judicial jurisdiction as an essential condition of the cloud service contract, is not defined;
-  Legal consequences of changing the country where information will be stored after the cloud service contract is signed by the cloud service providers or third parties whose property or services are used, are not regulated;












-  Control and oversight functions of public authorities in cloud services remain beyond legal regulation. Since cloud services are accompanied by risks in the field of information security, it is important to exercise government control over cloud services and the use of cloud computing technologies.

### **The Law of Ukraine «On Electronic Communications» Number 1089-IX of December 16, 2020. Becomes law on January 1, 2022.**
















The Law of Ukraine «On Electronic Communications», or the Law on e-Communications, establishes the legal framework for activities in electronic communications and on the radio frequency spectrum and defines the state's powers to manage and regulate electronic communications and the radio frequency spectrum. The law defines rights, obligations and principles of responsibility of natural and legal persons who participate in or use electronic communication services.

As already mentioned in the Section "EU Documents", the Law on e-Communications is an implementation act for fulfilling obligations stipulated in the Association Agreement with the EU and basic in the Roadmap for accession to the EU Single Digital Market. The implementation by EU authorities opens up the possibility for Ukraine to provide services and service providers, a treatment no less favorable than in the single market.

The Law on e-Communications stipulates:

-  Introducing registration of business entities engaged in activities in electronic communications;
-  Establishing an exhaustive list of requirements for market participants;
-  Initiating consultations with market participants on all issues affecting their interests;
-  Establishing a procedure for submitting documents to the regulatory body in electronic form;
-  Improving supervision in electronic communications to prevent offenses and reduce potential pressure on business entities, reducing inspections of these entities in their territory;
-  Defining fundamentals of preliminary regulation and the list of regulatory obligations that may be imposed on providers of electronic communications networks and services with a significant advantage in the market of certain electronic communications services and the regulatory authority to impose those obligations;
-  Establishing conditions for universal services, including price affordability, to provide access to the Internet and voice communications to the public;
-  Termination of activity of electronic communication service providers;
-  Liability for violation of electronic communications legislation;
-  Clearly defined rules for allocation and use of the radio frequency spectrum. In particular, references to objective, transparent, pro-competitive, non-discriminatory and proportionate radio spectrum policies and allocation can be found in the provisions on release of radio frequency spectrum;
-  Regulated issues of radio frequency spectrum trading and use, prevention of spectrum accumulation, prevention of cross-border radio interference, principles of neutrality of technologies and services and mechanisms to strengthen competition in the use of radio frequency spectrum. In addition, harmonizing the radio frequency spectrum in accordance with EU standards.

The shortcomings of the Law on e-Communications include the following:

-  Creation of a regulatory body and ensuring its independence are not foreseen. While the Law on e-Communications defines certain aspects of the national regulatory authority, or the NRA, it does not provide for establishment of the NRA as an independent body which is a primary requirement under the European Electronic Communications Code as established by European Parliament and Council Directive 2018/1972 of December 11, 2018 establishing the European Electronic Communications Code) (EECC, Articles 7 and 8) and a condition for granting the single market regime. Accordingly, there is uncertainty about establishing an independent NRA;
-  The authority of the NRA or legislatures to implement EU legislation aimed at implementing provisions of the EECC is not provided. The EECC empowers EU institutions to adopt implementing legislation;
-  Despite requirements of Article 45 of the EECC, the Law on E-Communications does not stipulate that service and technological neutrality should serve cultural and linguistic diversity and pluralism in the media. Perhaps these norms will be reflected in another draft law, such as the draft law on media – Number 2693 of December 27, 2019;
-  There is no mention of providing wireless broadband coverage of the national territory and population with high quality and speed and coverage of major national and European transport routes, including the trans-European transport networks;
-  The requirement related to harmonizing terms for assignment and use of harmonized radio frequency spectrum or the provision for 5G radio frequency spectrum is not foreseen. Implementation provisions and ongoing policy initiatives will be important;
-  Provisions governing authorization of the use of the radio frequency spectrum with the NRA or the Body of European Regulators for Electronic Communications, or the BEREC, are not foreseen;
-  It is recommended to expand provisions of the radio frequency spectrum;
-  Provisions for extraterritorial use of certain number ranges and coordination with the EU are not foreseen;
-  Provision of information on the pan-European emergency number and access to it needs to be improved;
-  Two items from the list of universal services are not defined;
-  Financing universal services, cost calculation and expenditure control require further improvement;
-  Anti-spam provisions contradict Article 7 of the GDPR regarding consent requirements;
-  A single information point for all passive infrastructure objects;
-  Rules to facilitate and coordinate construction work on infrastructure objects are not prescribed; and,
-  Mechanisms for out-of-court dispute resolution for all types of passive infrastructure.

20 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2018.321.01.0036.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG)

After the entry into force of this law, there may be a contradiction in terms of implementation and activities of NRA and their interaction with other cybersecurity regulators.

### **The Draft Law on the National Commission Administering State Regulation in Electronic Communications, Radio Frequency Spectrum and the Postal Services of Ukraine – July 9, 2020 – Number 4066.**

The draft law aims to define the legal status of the National Commission which regulates electronic communications, radio frequency spectra and the postal services of Ukraine.

The draft law contains addresses transparent appointment of members of the communication services regulator on an open competitive basis; independence of the communication services regulator in taking competent and fair decisions; openness of the state regulation process taking into account the Constitution of Ukraine and the decisions of the Constitutional Court in establishing the communication services regulator; and, appointment of its members among state authorities in Ukraine.



The draft law consists of four sections which establish specifics of the organization of the communications service regulator activity, its functions and powers and specifics of control on the market of electronic communications, radio frequency spectrum and postal services. The fourth section defines the final and transitional provisions, including the procedure for entry into force of this Law, taking into account the need to harmonize deadlines with the Law on e-Communications.

The draft law contains provisions that are contradictory and inconsistent with other legislation.

There is no certainty that the Communications Services Regulator is the only institution with the functions of a national regulatory authority and its powers will not overlap with those of the central executive authorities – the Ministry of Digital Transformation and the State Service of Special Communication and Information Protection, or the SSSCIP.

Also, Articles 13a and 13b of Directive 2002/21/EU<sup>21</sup>, as amended in 2009, which reference power of the regulatory authority to provide certain instructions to publicly available network providers, including timing of implementation to enterprises providing publicly available communication networks or publicly available electronic communication services, are not clearly implemented.

National regulators should have authority to require enterprises providing publicly available communications networks or publicly available electronic communications services:

-  To provide necessary information to assess the security and integrity of their services and networks, including a documented security policy; and,
-  To undergo a security audit conducted by a qualified independent national authority, and to provide results to the NRA. The cost of the audit must be paid by the business entity.

Business entities providing publicly available communications networks or publicly available electronic communications services should take appropriate technical and organizational measures to adequately manage risks associated with security of networks and services. These measures ensure a level of security appropriate to the risk presented. Measures must be taken to prevent and minimize the impact of security incidents on users and interconnected networks.

---

21 Directive 2002/21 / EU of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (as amended) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0021-20091219>






Business entities providing public communication networks are obliged to take all appropriate measures to ensure the integrity of their networks and ensure continuity of service delivery through these networks. Business entities must report to the competent NRA any security breach or loss of integrity that has had a significant impact on the operation of networks or services.

Eventually, the draft law will be finalized, but given the complexity of legal norms, this draft law should be consistent with the Law on e-Communications.

### **The Draft Law of Ukraine «On Amendments to Some Laws of Ukraine» (of November 13, 2020, Number 4378), submitted by the Cabinet of Ministers**

This draft law aims to regulate the issues of backing up information and data of state electronic information resources by state bodies, military formations created in accordance with the laws of Ukraine, state enterprises, institutions and organizations, as well as centralized storage of such backups at SSSCIP.

The draft law proposes:

-  To amend the laws of Ukraine «On the State Service of Special Communications and Information Protection of Ukraine» and «On the Basic Principles of Cybersecurity of Ukraine»;
-  To designate SSSCIP as responsible for maintaining backup copies of information and data of state electronic information resources;
-  Correct technical errors regarding the use of the terms “cybersecurity” and “cyberdefense”;
-  To supplement the terminology base of Ukrainian legislation with a definition of the term «state electronic information resources»;
-  To regulate the need to create backups and determine a list of organizations to which this norm applies. The Law of Ukraine «On Basic Principles of Cybersecurity of Ukraine» imposes the obligation to create backups for state authorities, military formations formed in accordance with the laws of Ukraine and state enterprises, institutions and organizations. The Law determines the procedure for transferring, storing and accessing backups determined by the Cabinet of Ministers. Implementing backup storage of information and data of state electronic information resources is a necessary and relevant step to create basic elements of cyberdefense of state electronic information resources and information infrastructure designed to process information whose protection is required by law.

Legislation points to the State Service of Special Communication and Information Protection of Ukraine for preservation of backup copies of information and data of state electronic information resources. Defining tasks for the public sector to establish procedures for transfer, storage and access to these copies is an important step to create an element of reliable protection. Such backup should provide the ability to perform emergency data recovery to neutralize consequences of an accident or data loss and ensure ability to take control of business processes. The backup should also resume critical functions in the shortest possible time using a reference backup.

The draft law “On Cloud Services” also contains requirements for backups, including when public users use cloud services, and introduces a definition of data processing center, or DPC.

DPC is a specialized technical area consisting of engineering systems of uninterrupted power supply, ventilation, cooling and humidity control, fire safety and physical security. It also addresses information,

electronic communication, software and hardware infrastructure, the facilities of which implement data storage and processing for providing cloud services, data backup, data transmission and rent communication racks.

Granting the State Service of Special Communications and Information Protection the responsibility to keep backup copies of information and data of state electronic information resources is likely to cause discussions, given the status of this regulatory body.

Among shortcomings of the draft law are lack of a definition of «criticality» of the very thing from which the obligation to transfer the resource for storage begins. There is no regulation of the procedures for transferring the resource for storage and the place of storage and the reverse order of using backup copies. The draft law will require substantial revision for the second reading in the Verkhovna Rada.

**The Draft Law on Amendments to the Criminal Procedure Code Regarding Improvement of the Effectiveness of the Fight Against Cybercrime and the use of Electronic Evidence (of 01.09.2020 Number 4004), submitted by Member of Parliament D.A. Monastyrskyi and others MPs.**

The draft law would amend Articles 7, 23, 60, 71, 84, 93 and 99 of Section I of the Criminal Procedure Code of Ukraine by adding the paragraph 4-1 on «Electronic Evidence»; Articles 104, 118, 123, 131, 132, 155, 157 of Section II of the Criminal Procedure Code by amending Chapter 15 on «Temporary Access to Things and Documents); Articles 171, 173, 177, 193, 234-237, 245, 252, 257, 264, 268, 290, 315, 322, 333, 358, 368, 374, 393, 549, 600; and, Article 39 of the Ukrainian Law «On Telecommunications».

The draft law attempts to enshrine use of electronic evidence in regulations governing the procedure for civil, commercial and administrative proceedings, supplement the Code of Criminal Procedure with provisions that define concepts and a list of electronic evidence, and generally is a consistent step in implementation of the Budapest Convention.

Amendments to the Code of Criminal Procedure of Ukraine concern:

- 1 Defining the concept and types of electronic evidence, supplementing the list of procedural sources of evidence, distinguishing the concept of electronic documents as a type of electronic evidence and other documents that are filed in electronic form;
- 2 Regulating special confiscation of virtual assets.

The draft law also proposes to make appropriate amendments to the Criminal Procedure Code of Ukraine, the Law of Ukraine On Telecommunications to improve effectiveness of the fight against cybercrime, concerning:

- 1 Improving the procedure for conducting covert investigative activities in criminal proceedings on cybercrime;
- 2 Improving public-private interaction between law enforcement agencies and telecommunications operators in administering operational and investigative activities, covert investigative activities and temporary access to information.





Authors of the draft law raised issues that need to be resolved. While introducing new mechanisms to combat cybercrime, they have not guaranteed rights and protected interests of persons from whom evidence should be seized. Contradictory legal constructions are proposed which provide definitions

in contradiction to the concepts of the legislation in electronic document management. This approach will lead to legal collisions and unequal application of definitions in civil and criminal law.

Subjects who will have access to electronic evidence should be controlled and the obligations of telecommunications operators and providers to transfer information should be clearly defined in method of transmission and storage of data. This ensures security of access to information from interference by an uncertain circle of people.

**The Draft Law on Amendments to the Criminal Procedure Code of Ukraine and the Code of Ukraine on Administrative Offences on Enhancing the Effectiveness of Counteraction to Cyberattacks (of 01.09.2020 Number 4003), submitted by Member of Parliament D.A. Monastyrskyi.**

The draft law proposes to amend Articles 36, 40, 41 and 110 of Section II of the CPC of Ukraine; amend Articles 131, 159 and 162 and add articles 1641, 1651 and Chapter 151 on «Urgent Storage of Information»). The legislation also proposes to amend Articles 236, 303 of the CPC of Ukraine, Articles 221, 255 of the Code of Administrative Offenses and Article 7 of the Law of Ukraine «On operational-search activity.” The legislation addresses

-  The possibility of temporary access to urgently stored information, which is not protected by the Law of Ukraine «On Protection of Personal Data» or not transmitted and stored under which participants of communication can rely on protection of information from interference by others. This is by order of a prosecutor or investigator and implements Article 17 of the Convention on Cybercrime. The proposed mechanism creates opportunities for abuse and requires stricter regulation. There are no mechanisms to protect the rights of the owner provided that when accessing electronic information systems, mobile terminals of communication systems and information and telecommunications systems without the permission of the investigating judge, it is also necessary to establish liability for disclosure;
-  The possibility of legally gaining access to computer systems that are physically located outside the search location to overcome logical protection systems, to obtain information on the specifics of computer systems and the protective measures applied to them (implementation of Article 19 of the Convention on Cybercrime) – the proposed mechanism creates opportunities for abuse, requires more stringent and clear regulation and establishes liability for disclosure of information;
-  Establishing administrative liability for failure to comply with a lawful order of the prosecutor, on storage of information, on temporary access to urgently stored information by supplementing the Code of Administrative Offenses of Ukraine with the new article 185-14, «Failure to comply with the lawful order of the prosecutor, investigator on urgent storage of information, on temporary access to urgently stored information». Further elaboration is necessary to eliminate duplication and excessive expansion of certain provisions of the Code of Administrative Offenses;
-  Changing the Law of Ukraine «On Telecommunications» (subclause 2 of clause 2 of Section II “Final Provisions” of the draft law) requires further elaboration and clarification to establish appropriate safeguards for protection and preservation of relevant information of Article 39 of the Law of Ukraine «On Telecommunications”.




**On Amendments to the Criminal Code and the Criminal Procedure Code of Ukraine Concerning the Delimitation of Jurisdiction Over Crimes Committed in use of Information and Telecommunications submitted by Member of Parliament A.P. Fedienko and others on July 17, 2020. Number 3897).**


The purpose of the draft law is to develop and implement cyberdefense mechanisms aimed at creating an effective national system of cybersecurity, improving legislation regarding introduction of enhanced criminal liability for crimes committed against critical information infrastructure objects and state information resources and assigning the investigation cybersecurity crimes to the Security Service of Ukraine.


The draft law proposes:


 Introduction of qualified types of such crimes as:


- Unauthorized sale or distribution of information with limited access, which is stored in information and telecommunications systems or media. (Article 361<sup>2</sup> of the Criminal Code of Ukraine);
- Unauthorized actions with information that is processed in information and telecommunication systems or stored in the media and committed by a person who has the right of access (Article 362 of the Criminal Code of Ukraine);

 Increased responsibility for the actions specified in paragraph 1 if they are committed in relation to critical information infrastructure;

 Article 363 of the Criminal Code of Ukraine supplemented with a provision according to which a violation of the requirements for cyberprotection of information and telecommunication systems or telecommunication networks, will be a crime;

 Section XVI of the Special Part of the Criminal Code of Ukraine supplemented with Article 363<sup>2</sup>, which will establish criminal liability for encroachment on a state information resource or other information, protection of which is established by law, communication or technological system of critical infrastructure;

 Increased liability in the form of fines for offenses established by articles 361, 361<sup>1</sup>, 361<sup>2</sup>, 362, 363 and 363<sup>1</sup> of the Criminal Code of Ukraine;

 Investigation of crimes committed in relation to critical information infrastructure to the jurisdiction of the Security Service of Ukraine given that these crimes pose a threat to the information security of the state, which is an integral part of the national security of Ukraine.

The project ensures implementation of an important task to bring the terminology of Section XVI of the Criminal Code of Ukraine in line with modern terms used in legislation on telecommunications and cybersecurity.

Changes regarding establishment of criminal liability for encroachment on communication or a technological system of critical infrastructure provide, among other things, a comprehensive approach to forming a legal framework for protecting critical infrastructure objects.



**On Amendments to the Law of Ukraine «On the Security Service of Ukraine» on Reforming the Activities of the Security Service of Ukraine (24.03.2020 No. 3196-1), submitted by Member of Parliament, A.Y. Ustinova and others.**

The draft law proposes a new version of the Law of Ukraine «On the Security Service of Ukraine», or the Law, and would amend legislative acts on activities of the Security Service of Ukraine, or the SBU.

The SBU will be endowed with authority in cybersecurity which is partially defined in the current legislation; but, would be more systematized.

Tasks will include counterintelligence protection of state sovereignty; constitutional order and territorial integrity; defense, scientific and technical potential; state cybersecurity and information security; and, critical infrastructure objects.

In the headquarters and territorial offices of the Security Service of Ukraine functional units should be established in a division of counterintelligence protection of cybersecurity and information security of the state.

The powers of the Security Service of Ukraine will include participation in measures to counter cyberterrorism and cyberespionage, assessing and readiness of critical infrastructure to possible cyberattacks and cyber incidents, providing a response to cyber incidents in state security.

The changes envisaged in the draft law «On Operative Investigative Activity» are not consistent with changes proposed to the draft law on critical infrastructure in terms of SBU authority.

It is also required to clearly coordinate and delineate responsibilities in intelligence, counterintelligence, cyberespionage and cyberterrorism between agencies whose functions address them.

**On Amendments to the Law of Ukraine «On the Security Service of Ukraine» on Reforming the Security Service of Ukraine (24.03.2020 No. 3196-D), submitted by Member of Parliament A.N. Zavitnevych and others.**

The draft law proposes to amend the Law of Ukraine «On the Security Service of Ukraine», or the Law and amend legislation on the activities of the Security Service of Ukraine, or the SBU.

The SBU would be vested with the following powers in the field of cybersecurity.

Ensuring state sovereignty, territorial integrity, independence, constitutional order and a system of state administration, security of the population. Ensuring political; economic; defense; information; and, scientific and technological potential. Ensuring cybersecurity and information security of the state; and, critical infrastructure objects.

SBU authority will include participation in the implementation of measures aimed at countering cyberintelligence of foreign countries and fighting cyberterrorism and cyberespionage.

The SBU will implement counterintelligence support of critical information infrastructure. These functions are detailed the Law of Ukraine «On Basic Principles of Cybersecurity of Ukraine» and are missing in the basic law regulating the SBU activities.

It is also required to clearly coordinate and delineate SBU authority, including in intelligence, counterintelligence, cyber espionage and cyberterrorism between state authorities. This is important, given that numerous changes proposed in the laws of Ukraine «On Counterintelligence», «On Combating Terrorism», «On the Basic Principles of Cybersecurity of Ukraine», «On National Security of Ukraine».

The proposed changes to the Law of Ukraine «On Operative-Investigative Activity» are consistent with changes proposed to the draft law on critical infrastructure, in terms of SBU authority.

The draft requires careful and detailed revision to avoid excessive empowerment of the SBU without safeguards of parliamentary and public control.

## Draft Bylaws

According to results of an anti-corruption assessment by the National Agency on Corruption Prevention, or NACP, it was determined that certain provisions of the draft resolution «Certain issues of independent audit of information security at critical infrastructure objects», or the draft resolution, contain corruption risk factors.

Independent audit of information security at critical infrastructure objects in the absence of a list of CI objects, procedures for certification of auditors and requirements for the CI audit may create conditions for the implementation of corruption schemes.



According to the NACP, sources of corruption risk are the following:

- «Establishing an obligation to conduct an independent audit of information security at critical infrastructure objects in the absence of a defined list of objects.
- Legal uncertainty for certifying information security auditors, requirements for determining qualifications of auditors and the criteria for their certification and the procedure for maintaining a list of certified auditors.
- Expanding the powers of the SSSCIP to maintain a list of certified information security auditors.
- Establishing frequency of audits for various critical infrastructure objects under uncertain criteria for classifying objects as critical infrastructure objects, general requirements for their cyber protection, including application of cyberthreat indicators.
- Exclusion from the list of critical infrastructure objects, which are subject to the draft resolution; and, small businesses that provide telecommunications services that do not meet requirements of the Law of Ukraine «On Basic Principles of Cybersecurity of Ukraine».
- Uncertain violation of the principle of legal certainty, regulation of information security auditors and report requirements which are prepared on the results of an independent audit”.<sup>22</sup>

The draft resolution provides for expansion of SSSCIP powers in terms of maintaining a list of certified auditors of information security not provided for by the current legislation. The procedure for adding certified auditors to a list is not regulated.

22 Conclusion of anti-corruption expertise of the draft resolution of the Cabinet of Ministers of Ukraine «Some issues of conducting an independent audit of information security at the objects of critical infrastructure» Publication date: October 2, 2020

<https://nazk.gov.ua/uk/documents/vysnovok-antykorrupciynoyi-ekspertyzy-proyektu-postanovy-kabinetu-ministriv-ukrayiny-deyaki-pytannya-provedennya-nezalezhnogo-audytu-informatsiynoyi-bezpeky-na-ob-yektah-krytychnoyi-infrastruktury/?hilite=>



#### NACP recommendations:

- Define a list of critical infrastructure objects;
- Approve requirements for information security auditors and their certification and recertification;
- Determine the procedure for maintaining a list of certified information security auditors;
- Eliminate the provision on non-application of audit requirements for small businesses that provide telecommunications services;
- Define a list of regulations governing duties of auditors in conducting an independent audit of information security objects;
- Define the term «information security» in the draft resolution;
- Specify references to standards establishing requirements for information security at critical infrastructure objects in the draft resolution.

Other draft bylaws are being prepared for publication or are contingent upon adoption of this act, which requires finalization and are listed in Annex A.

## Conclusions

To improve the legal framework, it is recommended to strengthen individual elements of ensuring cybersecurity in Ukraine.

The draft laws on electronic evidence require substantial revision.

Legislation should establish the content, provide a description of the timing and conditions of a crisis situation, mechanisms for overcoming crises in cyber space, crisis response measures for cyberthreats, and composition of response forces. Currently, the legal framework does not reflect mechanisms for cybersecurity crisis management.

The legal framework for information technology in public administration is outlined in the legislation on informatization, information protection in ITS and e-governance. But developing new legislation, given the lack of institutional memory makes it difficult to change long-standing policy and strategic documentation. Additional factors are created to unbalance the management system.

## Gaps and Ambiguities in the Current Legislation

Presidential Decree No. 96/2016<sup>23</sup> provides for development of a rapid response system to computer emergencies, which can be seen as a response to cyber security crises. However, rapid response can be administered both at the stages of eliminating deficiencies in the implementation of preventive cybersecurity measures and at subsequent stages of countering cyber aggression and identifying and eliminating cyber threats.

Solving problems of formation of legislation on crisis response in cyber space are proposed through the use of basic documents on cybersecurity while supplementing them with provisions for crisis response. Legislation can be improved on emergencies in terms of joint action in cyberthreats; information protection in information and telecommunications systems; civil protection; and, combating terrorism.

Analysis of the composition, content and scope of issues to be regulated by legislation on cybersecurity, counterterrorism, information protection and security shows that specific legislation better addresses issues within the competence of special departmental structures. Their task in the context of crisis response and cyberaggression is not coordinated in time and activities and the composition of crisis response forces and the procedure for their interaction are not defined. The structures to ensure operational management of combined forces during cyber aggression and crisis response are not in place.

Current cybersecurity legislation also does not require creation and use of information and analytical systems to support management decisions, including under conditions of crisis response.

Regulator participation in determining the CI according to criteria established by the act of the Cabinet of Ministers remain ambiguous. Regulators should be guided by law. This is especially true in the following areas: Financial, energy and digital services.

Issues of conformity of e-trust and cybersecurity services remain unresolved. The government has made no progress on these issues.

It should be noted separately that the procedure for preparing the acts far from transparent and public. Some acts are not published for a certain period of time even after their adoption at a Government meeting, thereby violating other legislation on access to public information and participation in the authorities' decision-making process.

Deadlines for implementation of acts, plans, and orders are either not set or are postponed due to non-fulfillment.

A separate issue that has remained unaddressed by the national government is the cooperation of central authorities with local governments, which have both their own mandate and that delegated to them by the national government. In terms of cybersecurity and cyberdefense, legislation does not provide an answer as to how cooperation will be administered.

The problem of self-regulatory organizations with delegated state functions – notary, advocacy and evaluation – is insufficiently studied and regulated. The complexity of regulation is that measures on interaction and cooperation should be introduced into laws regulating activities of such institutions. These statutes include the law of Ukraine «On Local Self-Government» and «On Notaries».

23 Decree of the President of Ukraine No. 96/2016 On Decision of the National Security and Defense Council of Ukraine of June 27, 2016 «On the Cybersecurity Strategy of Ukraine» <https://www.president.gov.ua/documents/962016-19836>

## Roadmap for Reforming the Cybersecurity Legal Framework

Over the past year, Ukraine has taken a number of positive steps to fulfill its international obligations and improve cybersecurity legislation. The most difficult stages remain for implementation – administering legislation and institutional changes, including new interaction mechanisms and preparing subsequent legislative changes.

Given the need to address issues in various areas, it is proposed to develop legislation: A law on cybersecurity (the concept of the future draft law that is proposed is already being discussed in the Working Group of the Verkhovna Rada's Committee on Digital Transformation); a draft law on critical infrastructure; a draft law to amend the Criminal and Criminal Procedure Codes to implement the Convention on Cybercrime; a draft law on cybersecurity regulator; and a draft law on information security.

It is also recommended to improve the system of cybersecurity in Ukraine: Development of a new system of cybersecurity management and coordination of system participants anchored in the law.

In Ukraine, there is no single body that can coordinate cybersecurity activities at the central level. The NSDC is the national security and defense authority under the President which coordinates and supervises activities of executive authorities in national security and defense in accordance with Article 107 of the Constitution of Ukraine.

Annex B specifies the authority of all statutorily defined institutions involved in cybersecurity.

According to the Cybersecurity Law, ensuring formation and implementation of policy in cybersecurity is the responsibility of the Cabinet of Ministers and the central executive body which ensures formation and implementation of state policy in organizing special communications, information protection, cybersecurity, telecommunications and use of radio frequency resources in Ukraine.

This special status body is directed and coordinated by the Cabinet of Ministers through the Deputy Prime Minister and Minister of Digital Transformation. But the peculiarity of this body is that it has a special status - it is a body of executive power, «is a component of the security and defense sector of Ukraine»<sup>24</sup> and cannot fully perform the role of the sector regulator, given its military element.

It is necessary to develop a new model of the system of cybersecurity and cyberdefense agencies with clearly distributed powers and a protocol of interaction between the components of the system in the executive branch and the security and defense sector.

There is also a need to develop a national target program on cybersecurity, which should provide both organizational and financial resources to ensure cybersecurity.

Changes in the law can be systematized into the following groups:

1. Review SSSCIP's Authority and Amend the Law Regulating It:

- Separation of security and defense from «civilian functions» and transfer of special communications to the competence of defense agencies;

<sup>24</sup> Law No. 3475-IV of February 23, 2006 on the State Service of Special Communication and Information Protection of Ukraine <https://zakon.rada.gov.ua/laws/show/3475-15>

- Separation of cybersecurity regulator functions from the SSSCIP to a new structure given financial situation of the national government;
- Leaving state control in the area of technical and cryptographic protection of information and supervision of critical information infrastructure facilities;
- Transferring competencies of the telecommunications regulator to the newly formed electronic communications regulator;
- Separate assessment of cybersecurity and trust services and transfer management to a self-regulatory organization which has yet to be established in the framework of a public-private partnership.

## 2. Draft Law on Cybersecurity:

- Aligns with European terminology
- Identifies a cybersecurity regulator or defining an organization with functions not burdened by a possible conflict of interest;
- Defines basic principles of interaction between cybersecurity actors, including their rights and obligations;
- Establishes the legal basis for self-regulation, the scope of its application and regulation of cybersecurity actors;
- Defines procedures for interaction, communication and exchange of information when a cyber incident occurs from CI objects to a single point of interaction;
- Defines requirements and tasks of computer security incident response teams;
- Defines procedure for accreditation in Ukraine and acceptance of accreditation of computer security incident response teams administered in the EU;
- Determines boundaries of the draft on activities related to processing of information constituting state secrets;
- Ensures periodic analysis of the effectiveness of measures related to cybersecurity of critical information infrastructure and state information resources by the personnel of these facilities and with involvement of authorized organizations in this field. This includes volunteer organizations accredited with established procedure;
- Defines general principles for conducting a national cybersecurity and critical information infrastructure review;
- Creates a legal basis for risk insurance, while identifying critical risks that should be insured; but, with a deferred deadline for training cybersecurity actors before introduction of insurance;
- Defines protection of certain types of information (for example confidential data and proprietary data), which should be expanded in the bylaws or in draft laws on information security;

- Determines the role of local governments in organizing tasks to ensure cybersecurity and CI protection;
  - Identifies challenges for the education and science system in terms of cybersecurity training and ongoing scientific observation of new trends in curriculum development for all age groups;
  - Clearly defines mechanisms of interaction between cybersecurity systems, the system of protection of personal data and exchange of information between regulators;
  - Defines requirements for activities of self-regulatory organizations with state delegated cybersecurity and data protection functions;
  - Identifies a national coordinator for international cooperation to combat organized crime, including cybercrime; and,
  - Pays attention to the final and transitional provisions which should synchronize other laws with the new cybersecurity law.
3. Finalization of the draft law on critical infrastructure.
4. Definition by law of the main types of digital services that are critical to national security while allowing the Cabinet of Ministers to determine requirements for technical regulations. Attention should be paid to reviewing requirements for protecting public (state, local government, self-regulatory organizations and institutions with state delegated functions, the judiciary and law enforcement) information and telecommunications systems and their interaction.
5. The cybersecurity strategy developed in 2016 until 2020 should be reviewed and analyzed for implementation. The new Cybersecurity Strategy should contain a separate section on network and information security, or two separate strategies should be developed. And the Network and Information Security Strategy should be developed in accordance with milestones, goals and indicators of achievement, as well as taking into account other ENISA<sup>25</sup> recommendations to ensure cybersecurity management effectiveness.
6. Other issues recommended to be implemented at the law or bylaw levels:
- Determining authority of the reformed Security Service of Ukraine;
  - Determining certification schemes for cybersecurity services;
  - Determining necessary measures for introduction of compliance assessment of information security management systems;
  - Conducting ongoing exercises for cybersecurity actors (including those in cybersecurity cyberdefense and cyberintelligence); and,
  - Locating and communicating data on vulnerabilities at critical infrastructure objects.

---

25 ENISA, recommendations for the preparation of national strategies <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>



## Annex A

# Legislation on Cybersecurity in Ukraine

### List of Ukrainian Laws

- 1 Convention on Cybercrime, ratified with reservations and declarations by Law of 07.09.2005 No. 2824-IV
- 2 Law No. 2163-VIII of October 5, 2017 On the Basic Principles of Cybersecurity of Ukraine;
- 3 Law No. 2229-XII of March 25, 1992 On the Security Service of Ukraine;
- 4 Law No. 2135-XII of February 18, 1992 On Operative Investigative Activity;
- 5 Law No. 3475-IV of 23 February 2006 On the State Service of Special Communication and Information Protection of Ukraine;
- 6 Law No. 80/94-VR of 5 July 1994 On the Protection of Information in Information and Telecommunications Systems;
- 7 Law No. 2657-XII of 2 October 1992 On Information;
- 8 Law No. 1280-IV of November 18, 2003 On Telecommunications;
- 9 Law No. 3855-XII of 21 January 1994 On State Secrets;
- 10 Law No. 2297-VI of June 1, 2010 On Protection of Personal Data;
- 11 Law No. 2469-VIII of June 21, 2018 On National Security of Ukraine;
- 12 Law No. 851-IV of May 22, 2003 On Electronic Documents and e-Document Flow;
- 13 Law No. 2657-XII of October 2, 1992 On Information
- 14 Law No. 2939-VI of January 13, 2011 On Access to Public Information
- 15 Law no. 74/98-VR of February 4, 1998 On National Informatization Program;
- 16 Law No. 75/98-VR of February 4, 1998 On the Concept of the National Informatization Program;
- 17 Law No. 3341-XII of 30 June 1993 On the Organizational and Legal Basis for Combating Organized Crime;
- 18 Criminal Code of Ukraine No. 2341-III of 5 April 2001;
- 19 Criminal Procedure Code of Ukraine No. 4651-VI of 13 April 2012;

## Bylaws on Cybersecurity in Ukraine

- 1 Presidential Decree No. 96 of March 15, 2016 On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016 On the Cybersecurity Strategy of Ukraine;
- 2 Presidential Decree No. 392/2020 of 14.09.2020 On the Decision of the National Security and Defense Council of Ukraine of September 14, 2020 On the National Security Strategy of Ukraine.
- 3 Presidential Decree No. 505/98 of May 22, 1998 On the Regulations on the Procedure of Cryptographic Protection of Information in Ukraine;
- 4 Presidential Decree No. 1229/99 of September 27, 1999 On the Regulation on Technical Protection of Information in Ukraine;
- 5 Presidential Decree No. 184/2015 of March 30, 2015 On the Decision of the National Security and Defense Council of Ukraine of March 12, 2015 On the Status of Overcoming the Negative Consequences Caused by the Loss of Material Carriers of Classified Information in the Temporarily Occupied Territory of Ukraine, in the Area of Anti-terrorist Operation in Donetsk and Luhansk Regions (for official use, not in public domain);
- 6 Presidential Decree No. 32/2017 of February 13, 2017 On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016 On the Threats to Cybersecurity of the State and Urgent Measures to Neutralize Them;
- 7 Resolution of the Cabinet of Ministers of Ukraine No. 1519 of October 11, 2002 On Approval of the Procedure for Providing Confidential Communication Services to Public Authorities and Local Authorities, State Enterprises, Institutions and Organizations;
- 8 Resolution of the Cabinet of Ministers of Ukraine No. 1772 of November 16, 2002 On Approval of the Procedure of interaction Between Executive Authorities on Protection of State Information Resources in Information and Telecommunications Systems;
- 9 Resolution of the Cabinet of Ministers of Ukraine No. 303 of May 14, 2015 Some issues regarding the organization of interagency information exchange in the National System of Confidential Communication;
- 10 On Approval of the Concept of Creating a State System of Critical Infrastructure Protection. Order of the Cabinet of Ministers of Ukraine No. 1009 of December 6, 2017.
- 11 On Approval of General Requirements for Cyberprotection of Critical Infrastructure Objects. Resolution of the Cabinet of Ministers of Ukraine No. 518 of June 19, 2019;
- 12 Some issues of critical information infrastructure facilities. Resolution of the Cabinet of Ministers of Ukraine, Order No. 943 of 09.10.2020
- 13 Certain issues of critical infrastructure objects. Resolution of the Cabinet of Ministers of Ukraine No. 1109 dated 09.10.2020
- 14 On Approval of the Technical Regulations for Cryptographic Information Protection Means, Resolution of the Cabinet of Ministers of Ukraine No. 991 dated October 21, 2020 (will enter into force on January 1, 2022)

- 
- 15 Procedure for inspection of the state of cyberprotection of critical information infrastructure, state information resources and information whose protection is required by law. Resolution of the Cabinet of Ministers of Ukraine No. 1176 dated November 11, 2020
  - 16 Some issues of ensuring the functioning of the system of vulnerability detection and response to cyber incidents and cyberattacks. Resolution No. 1295 of December 23, 2020
  - 17 On Amendments to the Concept of IT Centralization in Public Finance Management system. Order No. 215-r of 03.03.2020
  - 18 On Amendments to the Regulations on the Integrated System of Electronic Identification and the Regulations on the Ministry of Digital Transformation of Ukraine. Resolution No. 827 of 16.09.2020;
  - 19 On Establishment of Security and Information Protection Requirements for Qualified Electronic Trust Service Providers, as well as their registration points. Order No. 269 of 14.05.2020
  - 20 On Approval of the State strategy of Regional Development for 2021-2027. Resolution No. 695 dated 05.08.2020.
  - 21 On Approval of Amendments to the Regulation on Supervision of Payment and Settlement Systems in Ukraine. Resolution No. 11 of 21.01.2020
  - 22 On Approval of the Action Plan for Implementation of the Association Agreement Between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other hand. Resolution, Plan of October 25, 2017 No. 1106
  - 23 On Approval of the Regulation on the Definition of Critical Infrastructure Objects in the Banking System of Ukraine. Resolution, Regulation of 30.11.2020 No. 151
  - 24 On Approval of the Regulations on the Directorate of Strategic Planning and European Integration of the Ministry of Internal Affairs of Ukraine. Order, Regulation No. 406 of 21.05.2020
  - 25 On Approval of the Order on Inspection of the State of Cyberprotection of Critical Information Infrastructure, State Information Resources and Information, the requirement for the protection of which is established by law. Resolution, Regulation dated 11.11.2020 No. 1176
  - 26 On the Procedure of organizing the work and record keeping of the election commissions for the election of the President of Ukraine, People's Deputies of Ukraine, local elections. Resolution, Order of 10.08.2020 No. 173
  - 27 On Establishment of the Coordinating Council on Personal Data Protection. Order, Regulation of 09.07.2020 No. 88.15/20. Rev.: 10.08.2020.
  - 28 On the Strategic Plan of the Central Election Commission for 2020-2025. Resolution, Plan of 11.06.2020 No. 102
  - 29 On Approval of the Concept of Artificial Intelligence Development in Ukraine. Order, Concept of 02.12.2020 No. 1556-r
  - 30 On Approval of the Strategy for Combating Organized Crime. Order No. 1126-r of 16.09.2020.
  - 31 On measures to enhance the efficiency and transparency of territorial election commissions in organizing the preparation and conduct of local elections on October 25, 2020. Resolution of 02.10.2020 No. 331.
-

## List of Draft laws and Draft Bylaws

### The draft laws are registered in the Ninth Convocation of the Verkhovna Rada

- 1 The draft law on Critical Infrastructure (being prepared for registration)
- 2 On Amendments to Some Laws of Ukraine. The draft law of Ukraine, Map of the draft law passage of 13.11.2020 No. 4378
- 3 The draft law on Amendments to the Criminal Procedure Code of Ukraine and the Code of Ukraine on Administrative Offences on enhancing effectiveness of counteraction to cyberattacks. The draft law of 01.09.2020 No. 4003;
- 4 The draft law on Amendments to the Criminal Procedure Code of Ukraine on enhancing the effectiveness of the fight against cybercrime and the use of electronic evidence. The draft law of 01.09.2020 No. 4004;
- 5 On Amendments to the Law of Ukraine On the Security Service of Ukraine regarding reforming activities of the Security Service of Ukraine. The draft law of Ukraine of 24.03.2020 No. 3196-1
- 6 On Amendments to the Law of Ukraine On the Security Service of Ukraine regarding the improvement of the organizational and legal framework of the activity of the Security Service of Ukraine. The draft law of Ukraine of 21.10.2020 No. 3196-d
- 7 On Amendments to the Criminal Code and the Criminal Procedure Code of Ukraine (concerning the delimitation of jurisdiction over crimes committed in the use of information and telecommunications systems, networks and facilities. The draft law of Ukraine No. 3897 dated July 17, 2020;
- 8 On electronic communications. Law of Ukraine of 16.12.2020 No. 1089-IX (not in force)
- 9 The draft law on the National Commission carrying out state regulation in electronic communications, radio frequency spectrum and postal services of Ukraine, The draft law of 07.09.2020 No. 4066;
- 10 On Cloud Services. The draft law of Ukraine, Map of the draft law passage of 16.06.2020 No. 2655;
- 11 The draft law on amendments to some laws of Ukraine concerning preservation of backup copies of information and data of state electronic information resources of 13.11.2020 No.4378.



### Draft Bylaws

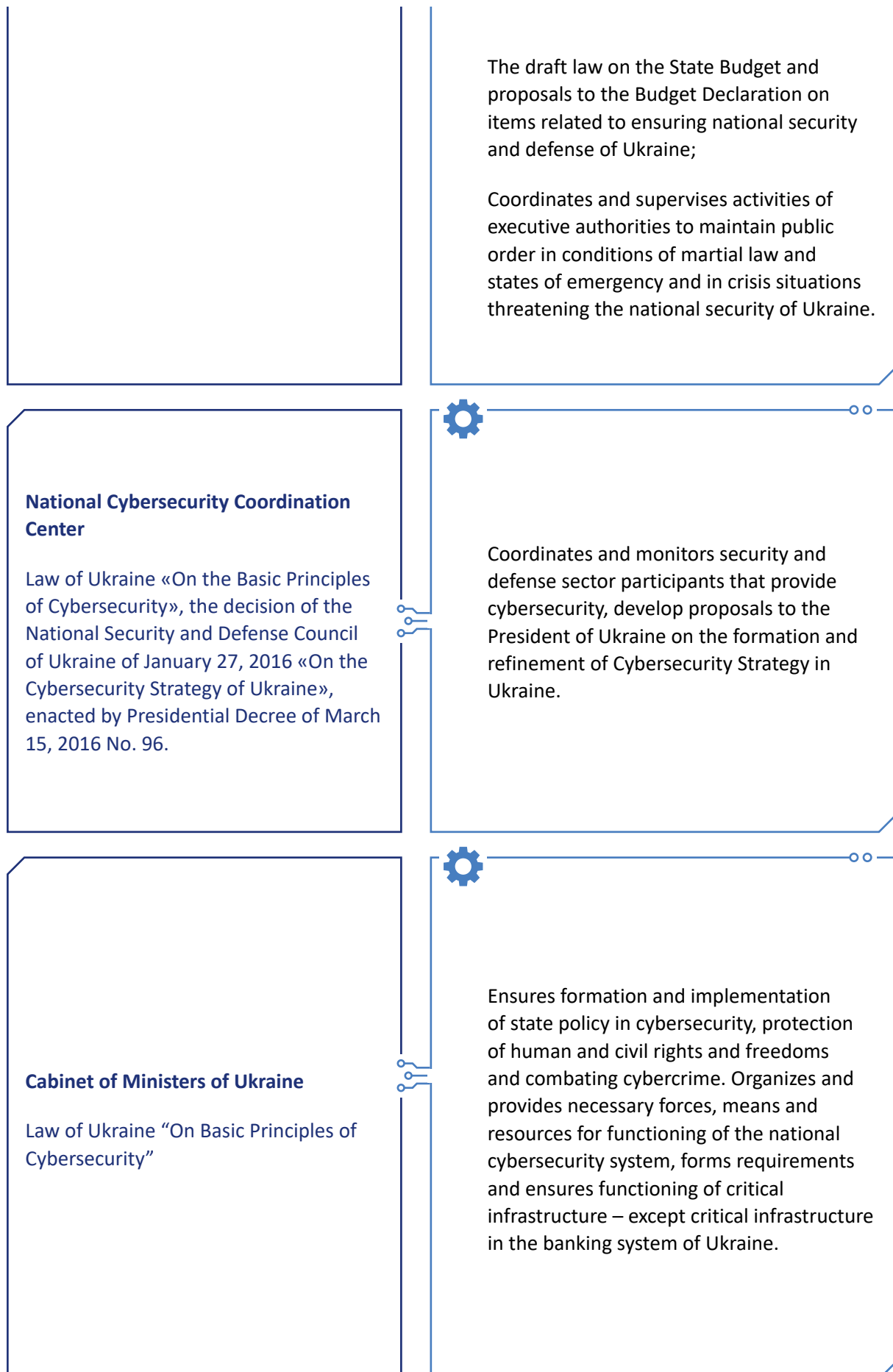
- 1 Resolution of the Cabinet of Ministers On Certain Issues of Functioning of the National Telecommunications Network (adopted at the Cabinet of Ministers meeting on December 17, to be published)
- 2 Resolution of the Cabinet of Ministers of Ukraine Certain Issues of Independent Audit of Information Security at Critical Infrastructure Objects (negative NACB conclusion to be adopted after the adoption of the law on critical infrastructure)

- 3 Order of SSSCIP On Approval of the List of National Telecommunications Network Services, Criteria and Methodology of Calculation of their Tariffing» (to be approved after the Resolution of the Cabinet of Ministers of Ukraine, Some Issues of Functioning of the National Telecommunications Network will come into force)
- 4 Decree of the President of Ukraine On Approval of Procedure for Cryptographic and Technical Protection of Classified Information (under discussion at the Office of the President of Ukraine).

## Annex B

### Institutions Responsible for Cybersecurity

Agency and Statutory Act Establishing the Authority	Functions in Terms of Cybersecurity
<p><b>The President of Ukraine, through the National Security and Defense Council of Ukraine</b></p> <p>Article 5 of the Law of Ukraine «On Basic Principles of Cybersecurity», Article 5 of the Law of Ukraine «On National Security»</p>	 <p>Implementation of cybersecurity coordination as a component of Ukraine's national security;</p> <p>Control over the security and defense sector</p>
<p><b>National Security and Defense Council of Ukraine</b></p> <p>Law of Ukraine «On the National Security and Defense Council of Ukraine»</p>	 <p>Develops issues related to national security and defense and submits proposals to the President. Decides on:</p> <p>Determination of strategic national interests of Ukraine, conceptual approaches and directions of national security and defense in the political, economic, social, military, scientific and technological, environmental and information areas;</p> <p>Draft state programs, doctrines, laws of Ukraine, decrees of the President of Ukraine, directives of the Supreme Commander-in-Chief of the Armed Forces of Ukraine, international treaties and other normative acts and documents on national security and defense issues;</p> <p>Improving the system of ensuring national security and organization of defense, formation, reorganization and liquidation of executive authorities;</p>



### **State Service of Special Communication and Information Protection of Ukraine**

The Law of Ukraine “On the Basic Principles of Cybersecurity”

Law of Ukraine “On the State Service of Special Communication and Information Protection of Ukraine”



Ensures formation and implementation of state policy on protection in cyber space of state information resources and information as required by law.

It regulates cyberprotection of critical information infrastructure and exercises state control in these areas. The law coordinates cybersecurity activities of other cybersecurity actors; ensures creation and operation of the National Telecommunications Network; implements organizational and technical model of cyberdefense; administers organizational and technical measures to prevent, detect and respond to cyber incidents and cyberattacks and eliminate their consequences.

The law informs about cyberthreats and appropriate methods of protection against them; ensures implementation of information security audits at critical infrastructure and establishes requirements for information security auditors. The law determines the procedure for their certification; coordinates, organizes and conducts security audits of communications and technological systems of critical infrastructure and ensures functioning of the State Cyberdefense Center and the Government Computer Emergency Response Team of Ukraine, or CERT-UA.

### **Government Computer Emergency Response Team of Ukraine, or CERT-UA**



- 1) Accumulates and analyzes data on cyber incidents, maintenance of the cyber incident state register;
- 2) Provides cybersecurity objects' owners with practical assistance in preventing, detecting, and remediating cyber incidents;



- 3) Organizes and conducts practical seminars on cyberdefense for national cybersecurity participants and owners of cyberdefense objects;
- 4) Prepares and posts website recommendations to counteract modern types of cyberattacks and cyberthreats;
- 5) Interacts with law enforcement agencies, ensuring they are informed, in a timely manner, of a cyberattack;
- 6) Interacts with international organizations on cyber incident response through participation in the Forum of Incident Response and Security Teams, or FIRST, with payment of membership fees;
- 7) Interacts with Ukrainian computer emergency response teams, and other businesses, institutions and organizations, regardless of ownership and activity engagement in activities related to the security of cyber space;
- 8) Processes information received from citizens about cyber incidents regarding cybersecurity objects;
- 9) Assists government authorities, the military and institutions and organizations regardless of ownership, as well as citizens of Ukraine in solving cyberdefense issues and counteraction to cyberthreats.



**Intelligence Agencies**

(Draft law on intelligence is being prepared)

Law of Ukraine "On the Basic Principles of Cybersecurity"



Administer intelligence activities in response to threats to Ukraine's national security in cyber space.

**National Bank of Ukraine**

The Law of Ukraine "On the National Bank",

The Law of Ukraine "On Basic Principles of Cybersecurity"



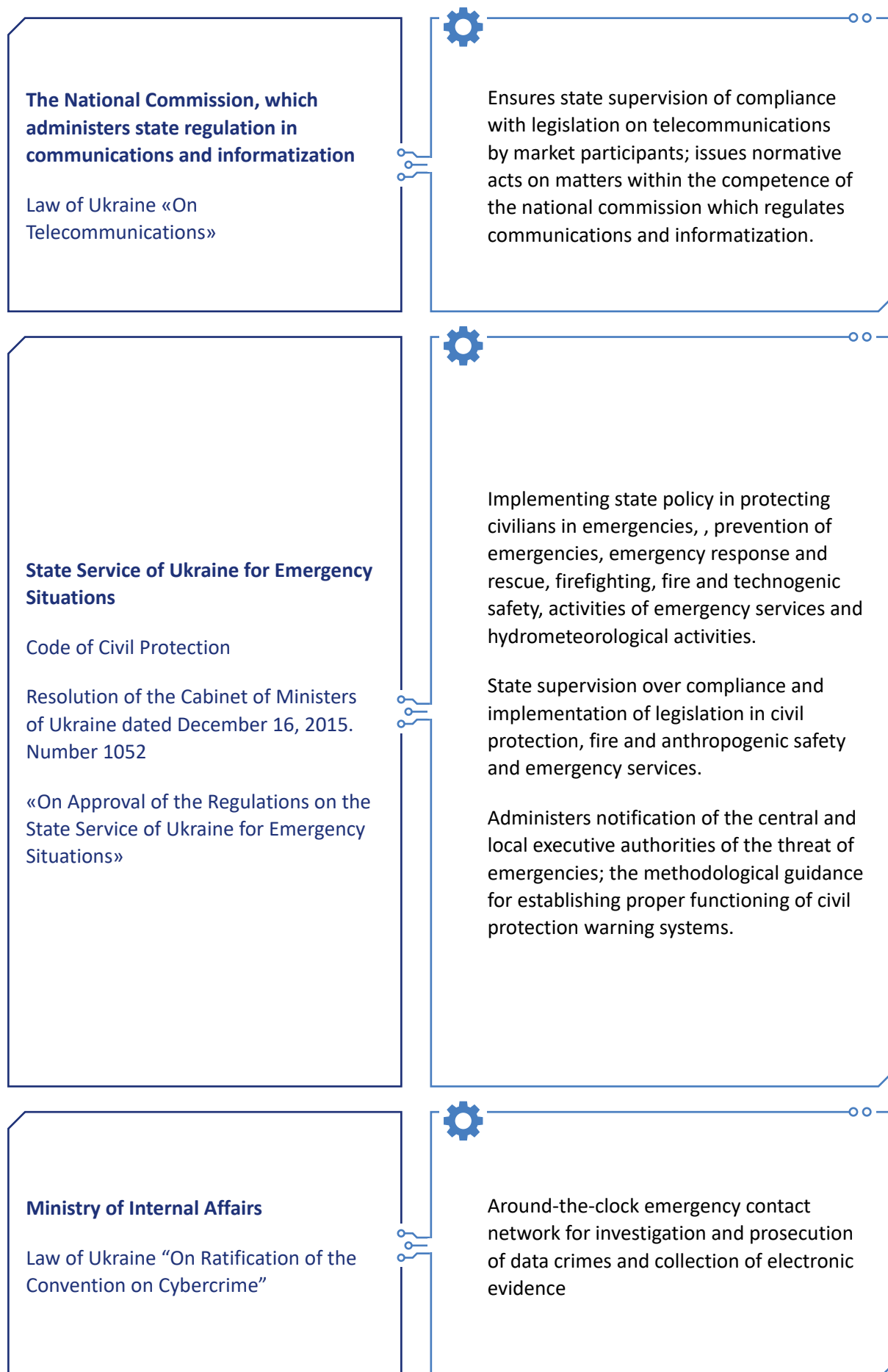
Defines procedure, requirements and measures to ensure cyberprotection and information security in the banking system and monitors fund transfers. Creates a cyberprotection center in the National Bank and ensures cyberprotection function in the banking system. Ensures cyberprotection status assessment and the audit of information security for critical infrastructure in the banking system.

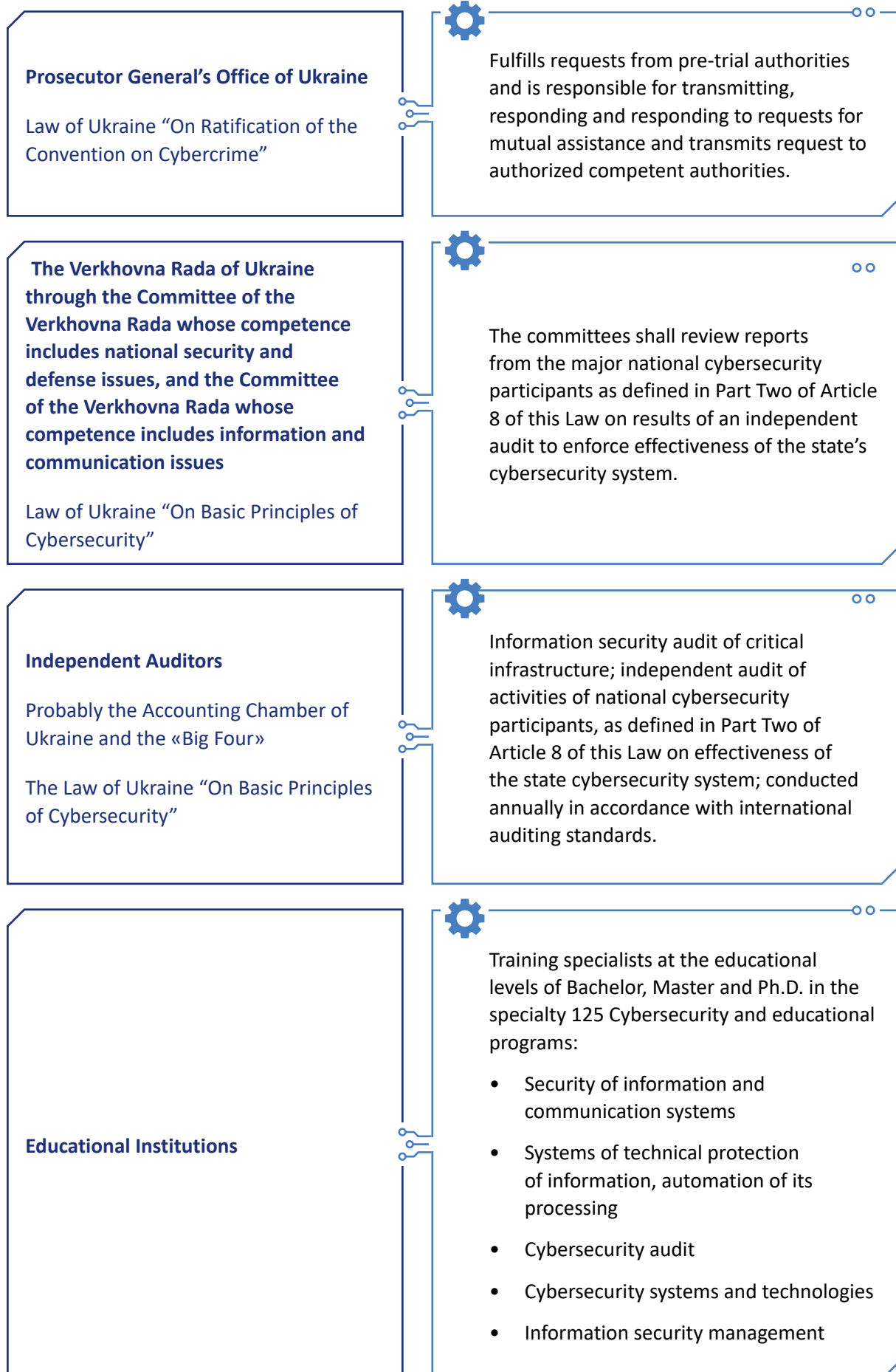
**Ministry of Digital Transformation**

Issues of the Ministry of Digital Transformation, resolution of the Cabinet of Ministers of Ukraine dated September 18, 2019. Number 856



Participates in: Forming state policy in cryptographic and technical protection of information; cybersecurity of telecommunications; use of radio frequency resources in Ukraine; special purpose of the government postal service; mandated protection of state information resources and information in telecommunications; use of state information resources to protect information, combat technical intelligence and functioning, security; and, developing the state system of government communications – the National System of Confidential Communications. It also developed and organizes state programs on information protection and cyberdefense.





### **Subjects Ensuring Cybersecurity:**

- 1) Ministries and other central executive bodies;
- 2) Local public administrations;
- 3) Self-governing bodies;
- 4) Law enforcement, intelligence and counterintelligence agencies. Subjects of operative and investigative activities;
- 5) The Armed Forces of Ukraine and other military formations formed in accordance with the law;
- 6) National Bank of Ukraine;
- 7) Enterprises, institutions and organizations classified as critical infrastructure objects;
- 8) Business entities, Ukrainian citizens and associations of citizens; other persons carrying out activities and/or providing services related to national information resources; information electronic services; implementation of electronic transactions; electronic communications; protection of information and cybersecurity.

The Law of Ukraine “On Basic Principles of Cybersecurity”



Implementation of cybersecurity measures to: Prevent the use of cyber space for military, subversive, terrorist and other illegal and criminal purposes; detect and respond to cyber incidents and cyberattacks and eliminate their consequences; information exchange on actual and potential cyberthreats; develop and implement organizational, educational and other activities in of cybersecurity, cyberdefense and cyberprotection; and, ensure information security audits, including at subordinate objects and objects that belong to their management





Global Expertise. Local Solutions.  
Sustainable Democracy.