USAID
FROM THE AMERICAN PEOPLE

USAID CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE

REVIEW OF THE REGULATORY FRAMEWORK FOR CRITICAL INFRASTRUCTURE CYBERSECURITY IN UKRAINE: LEGISLATIVE ASSESSMENT REPORT

This publication was produced by the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity under Contract No. 72012120C00002 at the request of the United States Agency for International Development. This document is made possible by the support of the American people through the United States Agency for International Development. Its contents are the sole responsibility of the author or authors and do not necessarily reflect the views of USAID or the U.S. Government.

Program Title:	USAID Cybersecurity for Critical Infrastructure in Ukraine
Sponsoring USAID Office:	USAID Ukraine
Contract Number:	72012120C00002
Contractor:	DAI Global, LLC
Submission Date:	November 16, 2020, resubmitted October 22, 2021
Author:	DAI Global, LLC

CONTENTS

ACRONYMS

CDTO	Chief Digital Transformation Officer
CEM	Cyber Excellence Mechanism
CERT-UA	Computer Emergency Response Team of Ukraine
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CII/ES	Critical Information Infrastructure and Essential Service Operators/Providers
CI Directive	European Union Directive on the identification, designation, and protection of European critical infrastructure
CIO	Critical Infrastructure Operator
CISO	Chief Information Security Officer
CIP	Critical Infrastructure Protection
CS	Cybersecurity
CSA	Cybersecurity Service Authority
CSIRT	Computer Security Incident Response Team
ECI	European Critical Infrastructure
ENISA	European Network and Information Security Agency
EU	European Union
GOU	Government of Ukraine
ICT	Information and Communications Technology
IFES	International Foundation for Electoral Systems
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
MDT	Ministry of Digital Transformation
MISP	Malware Information Sharing Platform
NATO	North Atlantic Treaty Organization
NBU	National Bank of Ukraine
NCIPC	National Critical Infrastructure Protection Commission
NCCC	National Coordination Center for Cybersecurity
NIS Directive	European Union Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
NIST	U.S. National Institute of Standards and Technology
NSDC	National Security and Defense Council
OCI	Objects of Critical Infrastructure

OCII	Objects of Critical Information Infrastructure
SBU	Security Service of Ukraine
SCPC	State Cyber Protection Center
SCSA	State Cybersecurity Service Authority
SISI	State Information Security Inspection
SO	Strategic Objective
SOC	Security Operation Center
SOP	Standard Operating Procedure
SSCA	State Special Communications Agency
SSSCIP	State Service for Special Communication and Information Protection of Ukraine
TISM	Threat Intelligence Sharing Mechanism
U.S.	United States
USAID	United States Agency for International Development
VPM	Vice Prime Minister

EXECUTIVE SUMMARY

This report provides an assessment and review of the **cybersecurity-related legal landscape** in Ukraine and recommends legislative, institutional, and operational improvements to increase the maturity of the national cybersecurity ecosystem. Together with other parallel efforts, the recommendations in this report will inform the development of Ukraine's cybersecurity legal instruments, ultimately shifting the country's reactive cyber sector into a proactive global cybersecurity leader.

This report identifies gaps in Ukraine's cybersecurity-related regulations and recommends new regulations as well as amendments to existing regulations to help close these gaps. The report also contains recommendations for the governance of key public cybersecurity actors, including for improving their technical and operational cybersecurity capabilities.

Key recommendations for improving Ukraine's cybersecurity legal landscape include the following:

1) Adopt regulation to reform the cybersecurity governance model in Ukraine to be more balanced between national security and civilian interests and inclusive of stakeholders from across the public, private, and civil sectors in cybersecurity policymaking.
2) Put in place policies, practices, and partnerships that build trust between public and private sector stakeholders not only to encourage information sharing on cybersecurity threats or incidents but also to enable sectors to effectively work together to solve national cybersecurity challenges through transparent governance mechanisms.
3) By effectively engaging a broader range of stakeholders, expand the vision and common understanding of cybersecurity as a strategic foundation that enables a stable and vibrant digital economy in Ukraine.

Policymakers embarking on the multi-year process of improving the current cybersecurity-related legal landscape and the national critical infrastructure cybersecurity ecosystem should rely on this report to identify regulatory and policy goals that are not only desirable but also *achievable* in Ukraine's current national cybersecurity ecosystem. This report informs the implementation of the National Cybersecurity Strategy, which was approved by Executive Order on August 26, 2021. This report also informs the development of the National Cybersecurity Roadmap to assist the Government of Ukraine (GOU) in implementing Cybersecurity Strategy.

INTRODUCTION

Ukraine has faced escalating cybersecurity incidents since the Revolution of Dignity in February 2014. The most severe incident occurred in June 2017, when Ukraine was ground zero for a global cyberattack. The NotPetya malware attack was designed to disrupt the operations of public and private entities in Ukraine on the eve of Constitution Day. NotPetya quickly spread to other countries and global businesses. The full cost of the attack is estimated to be as high as $10 billion, according to U.S. cybersecurity authorities.[1] In addition, countries around the world have seen an uptick in ransomware attacks, with critical infrastructure (CI) as one of the primary targets. In Ukraine, CI operators and public sector owners of critical information infrastructure (CII) face numerous challenges in effectively detecting, responding to, and recovering from cyber incidents. Both public and private entities have struggled to secure their systems as the frequency and sophistication of malicious cyber activities increase in Ukraine and worldwide.

The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (the Activity) is designed to reduce cybersecurity vulnerabilities in CI and transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader. To achieve this goal, the Activity will pursue the following strategic objectives (SOs):

[1] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

- **SO1:** Create a safe and trusted environment to accelerate the development of people, processes, and technology in support of cybersecurity across critical infrastructure sectors and assets in Ukraine.
- **SO2:** Strengthen Ukraine as a sovereign nation built on a secure, protected, and dynamic economy, supported by a talented pool of human capital.
- **SO3:** Stimulate demand for and supply of Ukrainian cybersecurity solutions and service providers to empower, equip, and finance cybersecurity entrepreneurs and businesses.

To support the implementation of SO 1, the Activity conducted this legislative assessment to review existing, drafted, and planned cybersecurity legislation, policies, and institutional reform strategies relevant to critical infrastructure protection and security.

PURPOSE AND OBJECTIVES

The purpose of this report is to assess and review cybersecurity legislation, policies, and institutional reform strategies relevant to critical infrastructure protection (CIP) in Ukraine.

The Activity reviewed and assessed the regulatory framework for establishing cybersecurity agencies, the minimum cybersecurity requirements for CI operators, the implementation of cybersecurity measures, cybersecurity audit requirements, and other issues enabling cybersecurity governance reforms.

The review identifies and highlights the major challenges to developing an efficient national cybersecurity system for CI in Ukraine.[2] Based on these challenges, the Activity proposes recommendations and next steps for developing the legal pillar of the Roadmap for National Cyber Resilience and associated regulations (Annex 2 Legislative Roadmap) in line with the European Union (EU) Cybersecurity for Critical Infrastructure Framework (Directive on Security of Networks and Information Systems [NIS Directive][3], the Critical Infrastructure Directive[4], and the EU Cybersecurity Act)[5].

The report proposes two complementary cybersecurity governance reform models for ensuring more transparent and distributed policy making. It also examines opportunities and challenges related to the implementation of the proposed cybersecurity governance reform models. These findings will serve as a basis for the legal pillar of the Activity's National Roadmap for Cybersecurity.

METHODOLOGY

The Activity reviewed laws, regulations, policies, and strategies on cybersecurity and critical infrastructure, including presidential decrees, Cabinet of Ministers resolutions, and Ukraine's National Cybersecurity Strategy.

The report uses standard European Network and Information Security Agency (ENISA)[6] terminology according to the EU NIS Directive. The comparative table with the identified discrepancies between the terminology used in the EU and Ukrainian legal frameworks is included in Annex 3.

The Activity employed the following methodology:

1. **Investigate**. Reviewed prior assessments, interviewed stakeholders, and analyzed the current regulatory landscape.

---

[2] There are several challenges addressed in the Activity's Roadmap for National Cyber Resilience drawn from this assessment and other research conducted by the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity, including the Cyber Excellence Mechanism (CEM) Assessment and Cybersecurity Incident Preparedness Assessment and Program Plan.
[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[4] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[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)
[6] https://www.enisa.europa.eu/

2. **Identify gaps between the current state of the cybersecurity regulatory landscape in Ukraine and best practices.** Analyzed the gaps identified in prior assessments, the merits or appropriateness of each recommendation, and researched whether each recommendation had been implemented.
3. **Recommend next steps.** Recommended potential regulatory and public policy proposals.
4. **Develop a regulatory and policy agenda.** Used recommendations to inform the organization of tasks around the legal pillar of Roadmap for National Cyber Resilience.

A note on terminology challenges

Some of the terms and concepts in this report are challenging to explain clearly because cybersecurity-related and legislation-related terms mean different things to different people. To ensure common understanding of the concepts used in this report, we have defined key terms. For the sake of clarity, below are three key definitions that this assessment used in its methodology:

1. **Legislation** – The Activity reviewed both (1) the cybersecurity-related legal landscape, i.e., laws, regulations, and related guidance, and (2) the national cybersecurity ecosystem in the context of the legislation that defines its components, including (a) the relationships among government cybersecurity stakeholders, (b) the governance structure for government cybersecurity stakeholders, (c) technical cybersecurity realities, and (d) operational cybersecurity realities.
2. **Laws and regulations** – Of the legal instruments in the Ukraine, the Constitution is the broadest and carries the most legal authority. Following the Constitution, laws carry the next-most legal authority and are more specific than the Constitution. Regulations carry less legal authority than laws and are typically more specific. In this report, the term "laws" refer to actual laws. The term "regulations" includes actual regulations as well as other legal instruments that are subordinate to laws or other regulations.
3. **Legal landscape** – This term includes not only laws and regulations but also other documents and practices that contribute to national cybersecurity ecosystem, e.g., the Cybersecurity Strategy or the distribution of responsibility among government agencies.

Further complicating matters is the fact that, in some cases, Ukrainian legislation adopts inaccurate definitions that contradict internationally recognized definitions. These definitional challenges can have far-reaching consequences. For example, contradicting definitions can complicate efforts to align Ukraine's cybersecurity processes with EU and other international standards. Annex 3 outlines the various terminology contradictions between EU and Ukrainian definitions.

In carrying out this assessment, the Activity coordinated with other programs that had previously assessed Ukraine's cybersecurity legal framework. To develop a historical perspective of the cybersecurity ecosystem, the Activity also conducted a desk review of the following assessments:

- International Foundation for Electoral Systems (IFES), Ukrainian Cybersecurity Legal Framework (2019)
- Blueprint Energy Solutions, Final Report on Cyber Security in the Energy Sector (2019)
- EU Delegation to Ukraine, EU Support to Cyber Legislation Final Report (2019)
- MITRE Corporation, Stakeholder Re-calibration and Election Security Engagements (2018)
- MITRE Corporation, Recommendations to the Government of Ukraine on Cyber Governance Reform (2021).

The Activity considered the merits of each recommendation in the prior assessments and determined whether the progress on implementing recommended reforms was made, to the extent the Activity agreed with the recommendations, and identified steps needed to close gaps. A summary of progress on implementing these recommendations is provided in Annex 1.

UKRAINE'S CYBERSECURITY REGULATORY FRAMEWORK FOR CRITICAL INFRASTRUCTURE

Ukraine's cybersecurity institutional framework focuses on national security and defense concerns at the expense of viewing cybersecurity as foundational to national wellbeing and prosperity. This focus reflects the influence of the ongoing hybrid information and cyber warfare against Ukraine by malicious foreign actors and a traditionally rigid security structure.

In conducting this assessment, the Activity found that a simple overview of the legal landscape was insufficient to fully understand Ukraine's legislative framework as related to cybersecurity for critical infrastructure. The challenges facing the cybersecurity legal framework are varied and include weak enforcement, unclear roles and authorities among governmental entities, and lack of capacity to effectively implement cybersecurity laws and regulations. To ensure the Activity has a comprehensive understanding of the cybersecurity ecosystem, this assessment highlights three distinct but interconnected components of Ukraine's legal landscape: (1) laws and regulations, (2) government institutions, and (3) technical and operational capabilities.

LAWS AND REGULATIONS

Ukraine's cybersecurity regulatory framework includes laws and regulations, presidential decrees, resolutions by the Cabinet of Ministers, and orders issued by cybersecurity stakeholders. Unfortunately, gaps in this legal framework, contradictory guidance, and vague terminology have weakened the enabling cybersecurity environment.

SUBSTANTIVE REGULATION

Cybersecurity law in Ukraine is derived from the Constitution, the *Law on National Security* (2018), the National Security Strategy (2020), and the Cybersecurity Strategy (2021).

Ukraine's National Security Strategy, "Security of a Man – Security of a Nation," defines a foreign and domestic policy to ensure the security of national interests, including cybersecurity. The focus of the strategy is deterring armed aggression, strengthening resilience to national security threats, and engaging key international partners (such as the EU, U.S., and international organizations like North Atlantic Treaty Organization [NATO]). The Strategy calls for establishing an effective, resilient CI security system based on a clear articulation of stakeholder responsibilities, including in public-private partnerships.

The President of Ukraine recently approved a new national Cybersecurity Strategy,[7] which provides a more comprehensive take on cybersecurity. This strategy extends beyond national defense to include economic prosperity and European integration. Developed by the National Coordination Center for Cybersecurity (NCCC) in coordination with other government entities, the Strategy outlines three strategic goals for the following years: (1) building deterrence potential, (2) achieving resilience, and (3) improving cooperation. Implementation of the strategy will enable the Government of Ukraine (GOU) cybersecurity stakeholders and CI operators to respond in a timely and effective manner to cyberattacks, ensure a regime of permanent preparedness for real and potential cyber threats, and detect and eliminate the preconditions for their occurrence.

The national cybersecurity regulatory framework includes several laws and regulations, such as the *Law on the Basic Principles of Cybersecurity of Ukraine* (2017) (*Cybersecurity Law*);[7] the *Law on Protection of Information in Information and Telecommunication Systems* (1994);[8] the *Law on the State Service for Special Communications and Information Protection of Ukraine* (2006);[9] the Ukase[10] of the President

[7] Enacted by the President of Ukraine's Ukase (Executive Order) on August 26, 2021 # 447/2021
[8] https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
[9] https://zakon.rada.gov.ua/laws/show/3475-15#Text
[10] *Ukase* is the GOU equivalent of a U.S. Executive Order.

"Position on the National Cybersecurity Coordination Center" (2016);[11] and the Cabinet of Ministers' resolution *"Issues of the Ministry of Digital Transformation"* (2019).[12]

The following sub-sections explain the functionality and gaps in each of these laws and regulations.

CYBERSECURITY LAW

The *Cybersecurity Law* views cybersecurity ("*kiberbezpeka*") not as a dynamic process that changes and adapts but as a constant state of safety. This perception has resulted in a cybersecurity framework that is less flexible and less capable of meeting the resilience definition under the National Security Strategy. In contrast, the recent *U.S. Executive Order on Improving the Nation's Cybersecurity* (May 12, 2021)[13] modernizes the U.S. federal government's cybersecurity approach by viewing the space as fluid and constantly changing. The executive order introduced a zero-trust security model that requires continuous verification of cybersecurity operations using real-time information from multiple sources to determine access and other system responses, protecting data in real-time within a dynamic threat environment.

The Ukrainian regulations' limited understanding of "security" ("*bezpeka*") has linguistic roots; "*bezpeka*" conveys both "security" and "safety." This is also a consequence of the post-Soviet information security legacy, including the domestic information security management certification framework, which establishes documented information assurance and maintenance policies without mandating risk assessments and constant improvements.

A limited understanding of the term "security" is reflected more broadly in the Cybersecurity Law*, which does not identify the five cybersecurity functions (Identify, Protect, Detect, Respond, and Recover).[14] The law institutes an artificial division between active measures ("cyber protection") and the more general concept of cybersecurity as safety.*

The law defines "cyber protection" as "a set of organizational, legal, engineering, and technical measures, as well as measures of cryptographic and technical information protection aimed at preventing cyber incidents, detecting and protecting against cyberattacks, eliminating their consequences, restoring integrity and reliability of communication and technological systems." These cyber protection functions are assigned to several government agencies defined in the legislation as "key subjects of the national cybersecurity system." This artificial division (including at the level of laws) between cybersecurity and cyber protection creates a strategic challenge to developing cybersecurity governance and establishing the cybersecurity framework for CI.

DRAFT LAW ON CRITICAL INFRASTRUCTURE

Even though the *Concept of the Establishment of a State System of Critical Infrastructure Protection* (CIP) was approved in 2017,[15] there is still a regulatory gap for governing CI security and resilience, including institutional and operational cybersecurity capacities at the national, regional, and sectoral levels.

The draft *Law on Critical Infrastructure (CIP Law)*[16] provides for the establishment of a national CIP system at the national, regional, sectoral, and local levels of infrastructure and their categorization depends on the level of criticality. Sectoral bodies (ministries) together with CI operators will categorize assets according to four categories of criticality: (I) especially important at the national level, (II) vital assets of regional importance, (III) important assets of local significance, and (IV) essential assets of local significance. There are also four modes of CI operation: (1) regular mode of operation; (2) standby and prevention mode; (3) crisis-response mode; and (4) post-crisis recovery

[11] https://zakon.rada.gov.ua/laws/show/242/2016#Text
[12] https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text
[13] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[14] https://www.nist.gov/cyberframework/online-learning/five-functions
[15] The *Concept for the Establishment of the State System of Critical Infrastructure Protection, Enactment of the Cabinet of Ministers of December 6, 2017 #1009*-p
[16] The draft *Law On Critical Infrastructure No, 5219 of March 9, 2021*

mode. The Cabinet of Ministers of Ukraine will approve the National CIP Plan and Regulations for the exchange of information.

The Cabinet of Ministers of Ukraine will establish the National Commission for Critical Infrastructure Protection (the Commission), a new collective regulatory authority with a chairperson and six members as staff. The Commission will keep a Register of Critical Infrastructure Facilities completed with data provided by sectoral bodies (ministries).

CI operators will oversee establishing and maintaining a management system for physical security and the security of operating systems and cybersecurity; developing and implementing internal plans on security and resilience, risk management procedures, and recovery plans; implementing cybersecurity controls; participating in information exchange; and upskilling personnel, among other things.

The cybersecurity requirements for CIP still need to be defined in an updated general law on cybersecurity, the draft of which is pending introduction to the Verkhovna Rada during the November 2021 session. The draft law establishes the regulatory framework.

The identified shortcomings[17] in the draft *CIP Law* were addressed with expert support from the Activity, which helped improve the law between its first and second hearings in the Verkhovna Rada of Ukraine. The Activity has provided technical assistance and expertise at the request of the Parliamentary Committee on Digital Transformation to ensure that the draft laws on CIP and cybersecurity are consistent and in line with the EU framework (CIP Directive, NIS Directive, and the EU Cybersecurity Act).

RESOLUTIONS ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE

The Cabinet of Ministers' resolution *Basic Requirements on the Cyber Protection of Critical Information Infrastructure* (2019) (*Basic Requirements*) defines the basic cybersecurity requirements for critical infrastructure operators (CIOs).[18] However, this resolution was adopted before the GOU had developed a procedure for defining CII assets; therefore, many of the entities affected by the new requirements were unaware that the resolutions pertained to them. The *Basic Requirements* can be applied only to CIOs that are officially defined by the draft *Law on CIP*. Therefore, the *Law on CIP* must set up criteria that allow GOU to define a list of CIOs to be governed by *Basic Requirements*. The GOU has taken steps to address these gaps. In October 2020, the Cabinet of Ministers of Ukraine approved two important regulations governing CIP related to the *Basic Requirements* resolution described above. These are Resolution #1109, "*Some Issues Related to Critical Infrastructure Facilities,"*[19] which provides a methodology for identifying and categorizing CI facilities by level of criticality according to potential impact at the local or national level in the case of operational failure*;* and Resolution #943, *"Some Issues Related to Critical Information Infrastructure Facilities,"*[20] which, similarly, provides a methodology for identifying CII assets and instructs the State Service for Special Communication and Information Protection of Ukraine (SSSCIP) to develop and maintain a register thereof.

These regulations are not comprehensive, as they define only certain aspects for the identification of CI facilities and CII assets. As such, the CIP Law will have to establish a regulatory framework for CIOs aligned with the EU Directives and best international practices.

The cybersecurity and critical infrastructure regulatory framework lacks adequate coordination across different government institutions. The GOU has identified numerous key cyber authorities and recognizes their roles in securing the national cyberspace, but it has not developed the mechanisms, structures, and processes that govern coordination among these stakeholders. The next section introduces the key GOU entities tasked with implementing cybersecurity policy, describes

[17] The Conclusion of the Chief Scientific and Analytical Department of the Apparatus of the Verkhonva Rada of Ukraine on the review of the draft *Law On Critical Infrastructure of April 23, 2021*
[18] *General Requirements on the Cyber Protection of Critical Information Infrastructure, Resolution of the Cabinet of Ministers of June 19, 2019 # 518*
[19] https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF
[20] https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF

the relationships between these actors, and breaks down the ambiguities and overlap in their assigned roles.

KEY GOVERNMENT INSTITUTIONS WITH CYBERSECURITY AUTHORITY

The cybersecurity and critical infrastructure regulatory framework of Ukraine lacks the clear roles and authorities to serve as a solid foundation for a well-coordinated structure across government institutions. The GOU's numerous key cyber authorities often play overlapping roles in securing the national cyberspace. Moreover, the mechanisms, structures, and processes governing coordination among these stakeholders are underdeveloped. This section introduces the key GOU entities tasked with implementing cybersecurity policies and regulations, describes the relationships between these actors, and breaks down the ambiguities and overlap in their assigned roles.

The current institutional cybersecurity ecosystem is centralized and focused on the cyber protection functions of a small number of government agencies, which are defined in the legislation as "key subjects of the national cybersecurity system."[21] Eight of nine such entities are national security, law enforcement, or military organizations: (1) the NCCC/National Security and Defense Council (NSDC), (2) SSSCIP, (3) the National Police, (4) the Security Service of Ukraine (SBU), (5) the Ministry of Defense, (6) General Headquarters of Armed Forces, (7) the Foreign Intelligence Service, and (8) the Border Guard. These organizations execute controls to fulfill cybersecurity requirements by public and private entities in the civilian sector, excluding banking and financial markets. The one non-security cybersecurity entity among key subjects of the national cybersecurity system is the National Bank of Ukraine (NBU), an independent cybersecurity sector regulator for banking, financial markets, and payment transaction services.[22] In addition to these nine entities defined under law, the Ministry of Digital Transformation (MDT) has increasingly asserted itself as a cybersecurity player, in part because the Vice Prime Minister for MDT oversees SSSCIP.

The reform of the SSSCIP led by the VPM will require a review of the functions assigned to key cybersecurity actors and clarification of the cybersecurity postures of MDT and other line ministries.

NATIONAL SECURITY AND DEFENSE COUNCIL (NSDC)

The main coordinating body for cybersecurity of CI and other areas covered by national cybersecurity policy is the NSDC, an advisory body to the President of Ukraine. The NSDC has established the NCCC as an operational body to coordinate and manage activities in the field of cybersecurity as a component of national security.[23] The *Law on National Security* has authorized NCCC to "prepare developing process" of the Cybersecurity Strategy of Ukraine.[24]

MINISTRY OF DIGITAL TRANSFORMATION (MDT)

The MDT, headed by the Vice Prime Minister in charge of digital reforms, is a central executive body that ensures the formation and implementation of state policy in digitalization, digital development, digital economy, digital innovation and technology, and e-governance

Since its creation in 2019, MDT has grown rapidly and proactively engaged in dialogue with GOU stakeholders and international partners on developing cybersecurity policies. However, its specific cybersecurity role requires clarification in law. In addition, and tied to a potential restructuring of the SSSCIP, precise distribution of key functions and powers from the SSSCIP to sectoral (market) regulators (such as MDT for digital service market, national regulatory commissions, or line ministries for CI sectors/markets, such as the National Energy and Utilities Regulatory Commission for energy and utility services) will help to address cybersecurity governance issues. Similarly, adequate

[21] *Law On Basic Principles of Cybersecurity in Ukraine of 05.10.2017 № 2163-VIII*
[22] *Law on Payment (Transactions) Services of 30.06.2021 № 1591-IX*; amended *Law On Basic Principles of Cybersecurity in Ukraine.*
[23] Presidential Decree on National Cybersecurity Coordination Center of June 7, 2016, No 242/2016;
[24] Article 31 of the *Law on National Security of Ukraine* of June 21, 2018 No 2469-VIII;

cybersecurity based on best practices can help resolve conflicting functions within individual agencies, including the SSSCIP.

***MDT's cybersecurity mission should be defined in law to remove any potential overlaps in authority and function**. Currently, there is only a reference in the secondary legislation that MDT "participates in the formation of state policy in the areas of cryptographic and technical protection of information, cyber protection, protection of state information resources and information, development and organization of state programs on information protection and cyber protection implementation."*[25]

STATE SERVICE FOR SPECIAL COMMUNICATION AND INFORMATION PROTECTION OF UKRAINE (SSSCIP)

The SSSCIP is a central executive body with special (hybrid) status as civilian and military tasks in charge of the implementation of special communication (classified and unclassified communications) and information protection (assurance). The main public cyber entity subordinated to the SSSCIP—the State Cyber Protection Center (SCPC), recently relaunched as the "UA30 Cyber Center"—serves as the national Computer Security Incident Response Team (CSIRT) (CERT-UA) and Security Operations Center (SOC) for all participants in the ecosystem. The SSSCIP is directed and coordinated by the Cabinet of Ministers of Ukraine through the Vice Prime Minister of Ukraine who also serves as the Minister of Digital Transformation.[26] The SSSCIP's civilian authority (Administration of SSSCIP) is in charge of coordination, regulatory, operational, and supervisory functions related to the non-military public and private CII (i.e., establishing requirements and conducting state information security inspections, providing binding instructions for improvements, certifying cybersecurity tools, and licensing cybersecurity service providers).[27]

The SSSCIP is an integral part of the security and defense sector (its employees are members of the military service). CERT-UA's status as a military unit makes the private sector less trusting of and confident in the unit and, therefore, less likely to exchange information with CERT-UA. This dual role for SSSCIP presents functional complications to its operations. Further study of and functional analysis is required to examine the best ways to deconflict the dual subordination and responsibilities.

***The private sector—including CI essential and digital service providers—is left out of the current formal governance model. As such, the ability of private companies to influence cybersecurity-related policy is limited.** The only private sector entities that directly interact with the SSSCIP are those formally represented in the Public Council at the SSSCIP.*

TECHNICAL AND OPERATIONAL CAPABILITIES

LEGAL FRAMEWORK FOR AUDITS

The Cybersecurity Strategy and the *Cybersecurity Law* prioritize the development and improvement of the state control system for the protection of information and a system for the *independent audit* of information security. The *Cybersecurity Law* indicates that the SSSCIP "ensures the implementation of information security audit at critical infrastructure facilities, sets requirements for information security auditors, determines the procedure for their certification (re-certification); coordinates, organizes and conducts audit of security of communication and technological systems of critical infrastructure objects for vulnerability." The *Cybersecurity Law* states that also SCPC "ensures audit of information security and the state of cyber security of critical information infrastructure." The *Cybersecurity Law* requires that the Cabinet of Ministers "define requirements and ensure the functioning of the information security audit system at critical infrastructure facilities (except for critical infrastructure facilities in the banking system of Ukraine)" and that the SSSCIP oversees the

---

[25] Enactment of the Cabinet of Ministers "*Issues of the Ministry of Digital Transformation*" of September 18, 2019, #856;

[26] The Scheme of directing and coordinating the activities of central executive bodies by the Cabinet of Ministers of Ukraine through the relevant members of the Cabinet of Ministers of Ukraine was approved by the *Enactment on Optimizing the System of Central Executive Bodies No. 879 of October 20, 2019*

[27] *Law on State Service for Special Communication and Information Protection of February 23, 2006 No 3475-IV*; https://zakon.rada.gov.ua/laws/show/3475-15#Text; *Enactment of the Cabinet of Ministers on the Administration of State Service for Special Communications and Information Protection of September 3, 2014 No. 411*

drafting of regulations for audits. The terminological confusion of the independent audit by private sector audit companies and state inspection performed by SSSCIP and/or SCPC should be addressed in amendments to the *Cybersecurity Law*. Ideally, the state inspection function should be separated from both entities and assigned to a specially designated public entity (State Information Security Inspection) in line with the requirements for distribution of the executive authority among different types of executive public bodies established by *Law "On Central Executive Authority Bodies" of March 17, 2011, No. 3166-VI.*[28]

The need to conduct critical infrastructure audits and determine the level of information security and cybersecurity preparedness is indicated by the "*Concept of creating a state system of critical infrastructure protection.*" The requirements for these audits have not been approved, so it remains unclear who should conduct them and according to which methodology.

The Cabinet of Ministers *Basic Requirements* has also established requirements for audits. The *Basic Requirements* are generally harmonized with the localized standard DSTU/ISO/IEC 27005. The owners of CI facilities must demonstrate compliance by *independent audit*. However, the *Basic Requirements* do not indicate who should perform such an audit or how (e.g., with what frequency and by what methodology).

In a survey conducted by the Activity, only 51 perfect of CI respondents indicated that they had conducted an independent cybersecurity audit. Of those that had conducted an independent audit, most of the respondents reporting have learned from the audits' findings.

Such audits are not public; therefore, it is impossible to understand compliance with the *Basic Requirements* or the long-term impact, if any, of the audits on the improvements of CI cybersecurity.

To ensure best practices implementation, the USAID Cybersecurity Activity has assisted the SSSCIP by training auditors to conduct diagnostic assessments and developing a Cyber Maturity Model (CMM). CI operators are meant to use the CMM to better understand their current CS posture and develop a plan to address vulnerabilities based on a risk-management approach.

LEGAL FRAMEWORK FOR STAFF TRAINING

Staff training (along with the technical support of specialized units) is a key element of an organization's readiness to respond to a cyberattack. The *Basic Requirements* require that the owner (or manager) of the CI should implement awareness and training programs for employees on information security issues and monitor the level of awareness on an annual basis. Despite these requirements, such programs have not been implemented.

In a survey conducted in support of the Activity's Incident Preparedness and National Program Plan 30 percent of CI entities indicated that their employees do not undergo such training. Training (of cybersecurity command and operational staff) is an exception to the rule and is not regulated.

In June 2021, a Working Group under the NSDC presented a draft concept to address the challenges in developing educational programs for CI staffing. The concept describes the demand in workforce for critical infrastructure security and defines a two-stage roadmap for addressing needs: the development of professional workforce standards and educational standards for 2021-2025; and establishment of the network of competence certification centers for 2025-2030.

[28] https://zakon.rada.gov.ua/laws/show/3166-17

The USAID Cybersecurity Activity has contributed to the discussions and drafting by proposing for adaptation NICE Workforce Framework for Cybersecurity (NIST SP 800-181)[29] and assisting with the development of local standards for cybersecurity professionals. The NICE Framework can serve as a best practices guide for defining categories of common cybersecurity functions, specialty areas of the cybersecurity workforce, and work roles comprised of specific knowledge, skills, and abilities required to perform cybersecurity tasks, including those related to CI cybersecurity.

LEGAL FRAMEWORK FOR CYBERSECURITY INFORMATION SHARING AND COORDINATION

While various legal acts are in force which regulate the exchange of information on cyber threats and incidents, the practice of exchange of this information is not efficient. In 2008, the GOU developed the "Procedure for coordinating the activities of public authorities, local governments, military formations, enterprises, institutions, and organizations regardless of ownership to prevent, detect and eliminate the effects of unauthorized actions on state information resources in information, telecommunication and information-telecommunication systems." This procedure applies to a limited number of participants in the national cybersecurity system that process "state information resources." It clearly defines the actions of entities falling within the scope of this procedure, the actions of the "Coordinator" (SSSCIP), and the restrictions on the Coordinator regarding the use of the received information. Interviews conducted by the Activity show that the mechanism is not used regularly.

Ukraine's Cybersecurity Strategy has identified the "insufficient level of information exchange between cybersecurity actors" as one of the main challenges in cybersecurity governance. To address this issue, the Strategy proposes several tasks, including building a network of computer emergency response teams and developing and implementing a mechanism for exchanging information between public authorities, the private sector, and citizens. It also includes protocols for joint actions, including the real-time exchange of information on detected cyberattacks and cyber incidents among cybersecurity actors.

The *Cybersecurity Law* regulates the coordination and exchange of information before and during cyber incidents (i.e., that the CI should immediately inform CERT-UA about cybersecurity incidents). The law stipulates that the functioning of the national cybersecurity system is ensured through "the exchange of information on cybersecurity incidents between cybersecurity entities in the manner prescribed by law" (though no legislation on such exchange currently exists).

While the law partially assigns the functions of information exchange to CERT-UA, it does not spell out CERT-UA's tasks, nor does it specify the sources from which the team should receive information about cyber incidents. Similarly, none of its tasks is related to forming an information exchange system for cyber incidents.

The law defines the task of "exchange of information between public authorities, the private sector and citizens on cyber threats to critical infrastructure, other cyber threats, cyber-attacks and cyber incidents" as part of public-private cooperation, without establishing any mechanisms for implementing such interaction. This oversight has virtually blocked the implementation of most of the tasks defined in the law.

In 2018, the SSSCIP began to develop a draft "Protocol of joint actions of cybersecurity entities, owners (managers) of critical information infrastructure during the prevention, detection, prevention, cessation of cyber-attacks and cyber incidents, as well as in eliminating their consequences," which concerned information exchange processes during all stages of cyber incident management (pre-crisis, crisis, and post-crisis). Although the draft document was meant to offer a comprehensive solution, it has several shortcomings:

- Vague provisions

[29] https://doi.org/10.6028/NIST.SP.800-181

- Lack of a clear procedure for exchanging information between cybersecurity actors and the requirement for such exchanges
- Lack of a clear procedure for joint action in the event of a cyberattack on CI.

Despite these shortcomings, the draft protocol does include some important provisions. For example, it requires CI entities and operators to form a threat model based on the assessment of cybersecurity risks (implementation of a risk-oriented approach) and to implement practical cybersecurity measures based on this analysis.

Information exchange—although only about cyber incidents and cyberattacks involving a critical information infrastructure facility—is addressed in the *Basic Requirements*. It requires the owner or manager of the CI facility to inform CERT-UA (and, as appropriate, the relevant industry or sector emergency response team) and the functional unit for counterintelligence protection of the state's interests at the SBU. However, clear guidance is lacking for such disclosures, including how to inform, what information to share, and when to share it.

*Established with the support of the USAID Cybersecurity Activity, the **Threat Intelligence Sharing Mechanism (TISM) Working Group** aims to build a community and trust across the GOU, the private sector, and independent experts, resulting in the exchange of threat information for identification, detection, and response to cyber incidents. The TISM Working Group has endorsed the common grounds for the development of regulatory framework: (1) the Malware Information Sharing Platform (MISP), a single open-source technical platform for the exchange of indicators of compromise, and (2) a Traffic Light Protocol to serve as a common taxonomy for the platform.*

RECOMMENDATIONS

Although the current *Cybersecurity Law* defines the roles of key cybersecurity players, overlapping functions and responsibilities among key entities have led to institutional conflict. Both SSSCIP and the NCCC purport to be the main coordination body for the GOU's cybersecurity work, causing confusion and reducing the overall effectiveness of collaboration and cooperation on cybersecurity issues. In addition, because the cybersecurity agencies (NSDC, SSSCIP) focus on national defense and security, it is unclear how civilian public and private sectors CI communities could benefit from cooperation. No governmental body has been designated to lead coordination on CIP to support and facilitate strategic collaboration and exchange of information among CI operators. Some coordination exists with CERT-UA in that it receives notifications of incidents from CI operators. However, the mandate of CERT-UA includes neither proactive communications nor cooperation with those operators.

The interests of CI entities have not been fully considered by the GOU, despite their critical importance. The existing regulation does not specify institutional mechanisms for involving CI operators in transparent policymaking processes; nor does it invite CI operators to share responsibility for cybersecurity, viewing them rather as objects (CI facilities) to be regulated. In general, the ability of non-state (private sector or civil society) actors to influence, develop, and improve public cybersecurity policy is very limited. Attempts to establish a partnership through a network of Public Councils (existing at all central authorities, including the SSSCIP) have proved ineffective. These councils typically analyze draft normative documents prepared by the state body under which the Public Council was established. In addition, not all major actors in the national cybersecurity system have such councils (for example, the NCCC under NSDC lacks a non-state component in its management model, although it has the option to create scientific and expert councils). The new frameworks should encourage self-regulation of private cybersecurity stakeholders and their participation in developing CI security and resilience policy.

Ukraine should consider establishing a government agency outside the law enforcement, intelligence, or military sphere to advocate CI security and serve as a forum for CI owners

***and operators to influence how the GOU deals with cyber risk**. This would highlight the importance of cybersecurity technology in supporting broader digital transformation, digital economy, and e-governance.*

Build strategic partnership and trust. The gaps in the regulatory and institutional cybersecurity framework have been compounded by the GOU's technical and operational deficiencies. Improving coordination between the public and private sectors should be central to the development of a resilient cybersecurity system. The benefits of increased coordination can be harnessed through sharing cyber threat information between commercial organizations and government agencies in a real-time, secure, confidential, and dynamic manner, increasing situational awareness, and reducing the impact on CI. This could be achieved through a network of sectoral SOCs/information sharing and analysis organizations (ISAOs), which could increase cyber capabilities and address specific CI sector needs. The Activity will support the development and implementation of a TISM by connecting and piloting Threat Intelligence Platforms (TIPs) at energy and banking sector facilities in line with the Cybersecurity Incident National Preparedness Assessment and Program Plan developed by the Activity.

The new framework should demonstrate to the private sector the benefits of entering public-private partnerships, including a more secure overall cybersecurity environment; early warning of cyber threats, detecting and analyzing threat information; continued advisory support to learn from experiences of other users, including from mature cybersecurity stakeholders; and joint action in the case of cyberattacks and cyber incidents, including response and recovery capabilities developed during national table-top exercises. It should also provide for cooperative engagement and mutual capacity building between public and private sector cybersecurity teams, including internship, apprenticeship, and mentorship programs as well as other professional development initiatives.

These recommendations should become part of the legal pillar of the Roadmap, which will assist the GOU in implementing the new Cybersecurity Strategy in line with the EU cybersecurity for critical infrastructure framework and best international practices.

RECOMMENDATIONS

Any new cybersecurity laws should take care to define responsibilities and ensure consistency of the regulatory framework to avoid conflicts and overlapping functions among cybersecurity authorities and stakeholders, define general requirements for conducting a periodic review of the national cybersecurity system governance model, evaluating its maturity, and implementing strategic goals.

Other top regulatory priorities include amending the *Cybersecurity Law*, adopting a *Law on Critical Infrastructure*, amending the *Law on SSSCIP*, and adopting additional required procedures in secondary legislation. These laws and regulations should be amended or designed to do the following:

- **Ensure that the terminology for the cybersecurity sector used in Ukraine aligns with international best practices.** Adjust existing definitions and introduce new terms common in legislation and EU and international standards in this area (Annex 3).
- **Define mandatory information and operational security requirements for CI operators**, including security risk assessment and management, business continuity planning requirements, **apply monitoring, auditing, and testing of their networks and information systems; and comply with international standards for information or information systems security,** etc.
- **Develop and approve cybersecurity requirements for CII as baseline security measures and define tiers above that baseline**, supported by incentives for exceeding the baseline standards via cyber maturity improvement plans at the organizational level.
- **Clarify the role of the SSSCIP/SCPC in implementing technical and organizational security measures in public sector CII** (e.g., e-governance infrastructure, public registries, etc.) and separate the conflicting functions of audit regulation, management, and supervision (inspection) within SSSCIP/SCPC;

- **Identify the role and place of the national regulator(s) of cybersecurity for CI with mandates to coordinate incident response and risk management while also setting rules and standards overseen by industry regulators to ensure compliance with the principles of cybersecurity in specific sectors/industries**; provide sector regulators with the authority to introduce sector-specific requirements based on the sector-specific risk assessment. The implementation of security measures requires some expertise in CI domains (finance, energy, transportation, etc.), which the SSSCIP currently lacks. Sector regulators can provide appropriate expertise on the sector-specific risk assessment and application of standards in specific technical or industrial environments.
- **Develop a national response plan for cyber incidents impacting CI with clear protocols for reporting incidents to CERT-UA and sector authorities** based on defined severity, including incident management procedures, coordinated actions, and disclosure requirements; establish requirements for the national CERT-UA and sector CSIRTs in line with the requirements prescribed in Annex I to the NIS Directive.
- **Develop a common taxonomy for cyber incident classification** used by CERT-UA, SBU, NCCC, sector authorities, and CI operators. A standard template for incident notification by CI operators would include the type of incident, the number of users affected or possibly affected by the incident, the duration of the incident, the affected (or potentially affected) region or area, and the extent of disruption of the service to other sectors; develop a public disclosure policy based on the severity and impact of the incident and following appropriate notification to CII/ES; i**mplement measures for voluntary vulnerability disclosure in CI sectors, proactive communication regarding current cyber threats, and response and recovery actions.**
- **Liberalize the market for cybersecurity services, including a shift from licensing for conformity and compliance to a notification procedure for registration as a designated CI entity; empower industry self-regulation and introduction of certification schemes in line with the EU Cybersecurity Act.** The global digital economy requires constant and efficient defense of digital assets. Compliance with cybersecurity requirements is becoming the precondition for entering the EU digital market. Ukraine's cybersecurity legislation should approximate the EU framework, specifically the NIS Directive, Cybersecurity Act, and the CI Directive. In addition, compliance with international information security standards (ISO/IEC 27k) should be the starting point for more advanced or sector-specific standards, the development of cybersecurity certification schemes for IT products, and stimulation of investments in domestic CI of essential and digital services based on risk assessment and cyber insurance.
- **Review public procurement legislation** to implement Cyber Supply Chain Risk Management requirements.
- **Adapt the NICE Framework**, which offers best practices in designing and implementing a cyber workforce development plan to train, upskill, and retain cybersecurity talent. In Ukraine, such a program could include free or low-cost cybersecurity training and education programs for veterans as well as tools and resources necessary to begin a cybersecurity career.

CONCLUSION

The assessment revealed a range of gaps in the current regulatory and institutional cybersecurity framework in Ukraine. Currently, Ukraine's cybersecurity framework suffers from three key deficiencies. First, gaps in the regulatory framework have weakened the enabling environment for cybersecurity. Specifically, the current cybersecurity legal framework lacks sufficient flexibility to respond and adapt to cyber threats and does not adequately define cybersecurity requirements for CI. Second, while numerous GOU agencies are tasked with contributing to cybersecurity initiatives, coordination among these stakeholders is limited and insufficient given the challenges. Finally, the laws underpinning functional cybersecurity audits and training are underdeveloped, significantly hindering the GOU's technical and operational cybersecurity capabilities.

To address these deficiencies and gaps in the cybersecurity legal framework, the Activity offered several recommendations designed to inform the development of the National Cybersecurity Roadmap (legal pillar) and the legislative agenda. Recommendations include developing new laws and regulations to support cybersecurity for critical infrastructure; restructuring Ukraine's cybersecurity legal framework around proposed new cybersecurity governance entities (CSA and/or Credit Information Companies Regulation Act Commission); and putting in place new laws and practices that encourage cooperation between different cybersecurity stakeholders, including the private sector and civil society.

In addition to providing technical assistance in designing and implementing these legislative improvements (legislative pillar), the Activity is addressing gaps and shortcomings in the technical, organizational, capacity building, and cooperation pillars of the National Cybersecurity Roadmap. These activities will improve coordination between cybersecurity stakeholders and build the technical and operational skills of cybersecurity professionals, including government employees. In turn, changes to Ukraine's cybersecurity legal framework will ensure that these improvements are sustainable.

ANNEXES

ANNEX 1: PROGRESS ON IMPLEMENTATION OF RECOMMENDATIONS

The Activity coordinated with other programs that previously conducted assessments of Ukraine's cybersecurity legal framework and conducted a desk review to develop a historical perspective of the cybersecurity ecosystem. The Activity considered the merits of each recommendation in the prior assessments and determined whether the progress on implementing recommended reforms was made, to the extent the Activity agreed with the recommendations and identified steps needed to close gaps. This annex reflects a summary of progress on implementation of recommendations provided in previous legal assessments.

Implementation	Description
Approve the list of critical sectors and subsectors as a priority legal measure Prepare SSSCIP guidance for the identification of objects of critical infrastructure and run a workshop for CIs and sectorial competent authorities on how to conduct the identification process in a harmonized manner Make sure that the Cabinet of Ministers' decision on establishment of critical sectors includes critical services Review draft decision of the Cabinet of Ministers on Criteria and Order for Assigning objects to Critical Infrastructure to approximate it with the EU NIS directive by: • adding provisions regarding review of the list of critical infrastructures every two years • reviewing and detailing the criteria for critical infrastructure identification by adding the number of users relying on the service provided by the entity concerned, the dependency of other critical sectors on the service provided by the entity, the impact that the incident could have in terms of degree and duration on economic and societal activities or public safety, the market share of the entity, the geographic spread with regard to the area that could be affected by an incident, the availability of alternative means for the provision of service provided by the entity, the provision of essential services in two or more EU states. Expand the definition of the object of critical infrastructure by including "that provides critical services as established by the Cabinet of Ministers' decision and has an establishment within the territory of Ukraine"	Resolution of the Cabinet of Ministers of Ukraine No. 1109 dated 09.10.2020 "*Certain issues of critical infrastructure objects*" and Resolution No. 943 of 9 October 2020 "*Some issues involving critical information infrastructure facilities*" provide for: • the procedure for assigning objects to critical infrastructure objects; • list of sectors (subsectors), basic services of critical infrastructure of the state; • methods of categorization of critical infrastructure objects.
Develop and approve a list of minimum mandatory information security requirements for critical information infrastructure taking into account the guidance document on the security measures for Operators of Essential Services produced by the EU Cooperation Group	The Cabinet of Ministers of Ukraine Resolution No. 518 of 19 June 2019 "*On approval of the General requirements for cyber protection of critical infrastructure*" has established minimum mandatory information security requirements for critical information infrastructure
Consider including measures related to supply chain security in the strategy. Supply chain cybersecurity refers to the secure design and manufacturing of ICT elements used by CI and CII operators. Measures to provide supply chain assurance may include supplier assurance frameworks for CI and CII operators and certification requirements or guidelines for supply chain risk management (e.g., access rules for manufacturers for updating the firmware)	Define mandatory information security requirements for CII objects, including security risk assessment and business continuity planning requirements, cybersecurity supply chain risk management, etc. Review public procurement legislation to implement Cyber Supply Chain Risk Management requirements

Adoption of the *Law on CI* and relevant secondary legislation. The *Law on Cybersecurity* and the *Concept of CI Protection* serve as a good start for the adoption of legislation governing CI protection. The adoption of secondary legislation could be considered a temporary option; however, there is a risk that operators of CI will not implement it properly Define what constitutes a serious incident for CII/ES Expand the legal mandate of the National Bank regarding CIs to include financial market infrastructures	
Harmonize the process of CII identification with the CI definition, the only distinction being that critical information infrastructures are networks and information systems that the critical infrastructures are dependent on. In such a way, those entities (CIs) that do not depend on network and information systems for the provision of the critical service will not fall within the meaning of the NIS directive, and security and notification requirements will not apply Consider including measures related to the establishment of critical sector-specific protection plans, including development and maintenance of a national/sectoral risk registry and continuous risk monitoring Establish a legal requirement for CII/ES to manage risks posed to the security of their systems and facilities; have incident management procedures and business continuity plans; apply monitoring, auditing, and testing of their networks and information systems; and comply with international standards for information or information systems security Assign SSSCIP the right to issue binding instructions to the objects of critical infrastructures to remedy deficiencies identified during the audit	Establish legal requirements for CII/ES to manage risks to the security of their systems and facilities; develop business continuity plans; apply monitoring, auditing, and testing of their networks and information systems; and comply with international standards for information or information systems security
Introduce changes to the *Law on Basic Principles of Cybersecurity* in Ukraine by defining who is responsible for the approval of mandatory information security requirements for objects of critical information infrastructure, including security risk assessment and business continuity planning requirements Include measures related to the development of baseline security requirements for CIIs and make sure to align them with NIS directive requirements, including baseline security measures, risk assessment, user awareness, incident response and reporting, and business continuity measures High-level cyber incident management exercises and participation of decision-makers therein could be a mandatory requirement set in one of the laws or Cabinet of Ministers' decisions Develop a procedure and report format for informing the affected EU Member States, if the incident at CII/ES has an impact on two or more EU member states, bearing in mind that the security and commercial interests of the object of CII/ES and confidentiality of the information provided in its notification needs to be protected	Develop and approve cybersecurity requirements for CII as baseline security measures and define a series of tiers above that baseline, supported by incentives for exceeding the baseline standards via cyber maturity improvement plans at the organizational level

Clarify the role of SSSCIP regarding implementation of technical and organizational security measures in all critical information infrastructures to dispel the potential understanding that SSSCIP will provide appropriate and proportionate technical and organizational security measures to all Cis	Clarify the role of SSSCIP regarding the implementation of technical and organizational security measures in public sector CII (e.g., e-governance infrastructure, public registries, etc.)
Update legislative and organizational measures for CIP by requiring CIs to report only serious incidents to CERT-UA and possibly sectorial competent authorities	Develop a national response plan for cyber incidents impacting CI with clear protocols for reporting incidents to CERT-UA and sector authorities based on defined severity, including incident management procedures, coordinated actions, and disclosure requirements;
Develop notification guidelines on circumstances in which critical infrastructures are required to notify incidents, the format and procedure of such national notifications. Align these guidelines with the Cooperation Group guidelines	
Develop a standard template for incident reporting, which would require providing information on the type of incident, number of users affected by the disruption of essential service, the duration of the incident, and the geographical spread/ area affected by the incident, if any other countries are affected	
Develop a procedure and report format for informing the affected EU Member States, if the incident has an impact on the provision of essential services to other EU Member States, bearing in mind that the security and commercial interests of the object of critical infrastructure and confidentiality of the information provided in its notification needs to be protected	
Develop a procedure for informing the public about individual incidents, after notification of the incident by the digital service provider, if public awareness is necessary to prevent an incident or to deal with an ongoing incident	
Consider including measures related to national cyber contingency planning, i.e., how Ukraine would respond and recover from major incidents within CIIs. It does not need to be specific in strategy per se; but can include measures related to the development of national cyber security contingency plans as part of the overall national contingency planning, testing of the plans, training of personnel, and running of exercises. Also, it would be good to define in the strategy leading agencies responsible for cyber-crisis at CIIs management	
Develop a procedure for informing the public about individual incidents, after notification of the incident by the object of critical infrastructure, if public awareness is necessary to prevent an incident or to deal with an ongoing incident	
Update legislative and organizational measures for CIP by defining what constitutes a serious incident and harmonizing this definition with the EU's understanding	Establish requirements for the national CERT-UA and sector CSIRTs
Define the role of CERTs in both the public and private sectors. Consider assigning responsibility for the monitoring of CIIs, information sharing, early warning to CERT-UA	

Document and adopt incident and risk handling procedures based on ENISA's guidelines and recommendations of NIS Co-operation Group	
CERT-UA (and SBU to a lesser extent) should prepare a yearly National Cybersecurity Situation Report on incidents and threats	
Critical information infrastructure owners, when reporting and managing incidents together with national authorities, should use the same criticality categories and associated response times	
In a cyber crisis, additional incident management policies should be available for CERT-UA, such as the ability to request network or system isolation	
National cyber security incidents classification has to ensure that different sectors and organizations use the same terminology and there is no need to "translate and remap" in case of information sharing or joint investigations	
Incidents in different importance categories of CII can't be treated equally, an incident criticality metric should be developed and applied. This, in turn, will allow CERTs and coordination centers to prioritize their efforts, and this will lead to more effective national cyber situation assessment and crisis management	
A separate legal act related to "regional" and\or "national" cybersecurity incident category management will simplify the identification of such cases and allow setting specific processes for large-scale cybersecurity incidents management at all levels of cyber responders, will allow a seamless integration into existing crisis management processes	
Empower CERT-UA and other Ukrainian CERTs with sufficient capabilities to coordinate cyber incident management and conduct cooperation with public CERTs of other countries. Consider harmonizing CERT-UA and other Ukrainian CERTs' data handling practices with EU data protection legislation. It would help to establish trust with their constituencies and international fora that personal data handling, processing, and protection follow good standards	
Develop a common taxonomy for cyber incident classification to be used by CERT-UA, SBU, sectorial competent authorities, and Cis	Develop a common taxonomy for cyber incident classification to be used by CERT-UA, SBU, sector authorities, and CI operators
Develop a common taxonomy for cyber incident classification to be used by CERT-UA and CII/ES	
Develop a standard template for incident notification by CII/ES, which would require providing information on the type of incident, number of users affected by the incident, the duration of the incident, and the geographical spread/ area affected by the incident, the extent of the disruption of the functioning of service, and whether any other countries are affected	
Define CII/ES in the legislation, taking into account jurisdictional requirements	Identify the role and place of the national regulator(s) of cybersecurity for CI with mandates to coordinate incident

	response and risk management, while also setting standards for proactive cyber management
Run a national risk assessment on CIIs to establish a common understanding of risk factors that the nation faces. It should include an assessment of the threats towards Ukrainian CIIs and vulnerabilities (impact and likelihood). The result of a national risk assessment would be an overview of risk factors and their expected impact and likelihood of occurrence. Each risk identified and assessed in a national risk assessment can be consequently managed by an integrated national approach to risk prevention, preparedness and response Consider establishing a requirement for a CII/ES to have its main establishment in Ukraine or designate a representative in one of the EU countries where the services are offered	
Establish a legal requirement for CII/ES to report serious incidents to CERT-UA	Implement measures for voluntary vulnerability disclosure in CI sectors, proactive communication regarding current cyber threats, and response and recovery actions, and define the mechanisms for interaction, notification, and the exchange of information inside the cybersecurity ecosystem and with the community at large
In the legal framework, grant SSSCIP the right to conduct ex-post supervisory measures when provided with evidence from another EU Member State that a CII/ES does not meet security requirements Develop notification guidelines concerning the circumstances in which CII/ES are required to notify incidents, as well as the format and procedure of such national notifications	Review and redefine SSSCIP functions as an actor in the security and defense sector of Ukraine
In the legal framework, define the conditions when administrative fines can be issued to a legal person for failure to comply with the legal provision regarding the security of network and information systems and set ceilings for such fines Define who will be monitoring the implementation of the national cybersecurity strategy of Ukraine. According to cybersecurity governance set up in Ukraine, monitoring and evaluation of the national cybersecurity strategy could be performed by two institutions: (1) Council of National Security and Defense of Ukraine, which develops proposals for the President on the cybersecurity strategy of Ukraine and acts as a coordinator of activities in the field of critical infrastructure protection; or (2) Cabinet of Ministers as an implementer of national policy in the field of cybersecurity and provider of resources for the functioning of the national cybersecurity system Establish clear reporting mechanisms on implementation of the strategy (who reports to the Council of National Security and Defense of Ukraine and how often)	Define general requirements for conducting a periodic review of the national cybersecurity system governance model, evaluation of its maturity, and implementation of strategic goals.

Assessment of Cybersecurity Strategy Implementation. The Cybersecurity Strategy was adopted in 2016 and since then there has been no evaluation of its implementation. As the strategy itself does not define measures and tools for assessing its effectiveness, authorities have not assessed its implementation Development of the Cybersecurity Strategy 2020–2025 and Strategic Plan. SSSCIP considers the current Cybersecurity Strategy as effective between 2016–2020 as it was adopted in accordance with the National Security Strategy of Ukraine which ends in 2020. It would be timely to update the strategy and develop and approve a strategic plan for the same period, and for the future Set a specific timeframe for strategy implementation (for example, five years) Develop a strategy implementation plan with specific, time-bound, and measurable actions and resource their implementation adequately. Each strategic action should have a metric to monitor the progress made and the achievement of strategic goals. Also, each strategic action should have a designated responsible agency for its implementation Review the national cybersecurity strategy of Ukraine and include provisions into the strategic objectives regarding the protection of critical sectors of the national economy as per the NIS Directive	
Consider running a national cybersecurity capacity assessment to identify gaps, weaknesses, and strengths in Ukrainian cybersecurity capacity to inform the review of the strategy and development of actions. The value of a national cybersecurity capacity assessment is that numerous stakeholders from the public and private sector, academia, NGOs, and international organizations are brought together to discuss the most pertinent national cybersecurity issues and agree on a way to address them Include new actors with the role of CIP in the national cybersecurity strategy governance framework and define their mandates and tasks in initiating or developing cybersecurity policies and regulations and explain how they interact with the cyber security strategy owner(s). Specifically, define who is responsible for national cyber risk management, threat assessment, responding to critical situations, relevant stakeholder engagement, and international cooperation	Define general principles for conducting a review of the national cybersecurity system
Consider prioritizing the protection of certain critical sectors, which have a higher degree of awareness for cybersecurity and available resources. These sectors can provide a positive example to other critical sectors at a later stage Consider including measures related to the provision of tools and guidelines to support the implementation of risk management at CIIs. This can also include the provision of information on cybersecurity threats to Ukraine and its critical infrastructures.	Implement risk management requirements in CI sectors based on sector-specific risk
Approach and involve stakeholders, especially private actors, in the early stage of strategy development. This could help to increase their willingness to participate and voice their concerns. A good platform for private stakeholder engagement could be either through SSSCIP or a newly established State Service for Critical Infrastructure Protection	Establish institutional mechanisms for the engagement of key cybersecurity stakeholders in dialogue with CI operators, cybersecurity service providers, the professional cybersecurity

	community, and experts (including in the form of expert or advisory councils)
Organize focused workshops with senior officials and politicians regarding the value of cybersecurity for a modern digital economy and society and EU cooperation Create a national register with accredited cybersecurity experts that can be used for cybersecurity training and education programs	
Consider creating a national vulnerability database and building an early warning system for CIIs	Implement measures for voluntary vulnerability disclosure in CI sectors, proactive communication regarding current cyber threats, and response and recovery actions, and define the mechanisms for interaction, notification, and the exchange of information inside the cybersecurity ecosystem and with the community at large
Include measures related to public-private partnership establishment, as critical services are provided by the private sector in Ukraine. Public-private partnerships should address the security and resilience of CIIs and be used as a tool to pool expertise and resources of the private and public sectors together. As public-private partnership is at a very early stage in Ukraine, the most suitable goal of it could be information sharing and pooling capabilities to respond and recover from cyber incidents Facilitate the establishment of a platform for R&D in cybersecurity, which could take the form of public-private partnership and co-ordinate research and development in cybersecurity to meet public and private sector needs Adoption of the *Law on Public-Private Partnership on Cybersecurity*. The *Law on Cybersecurity* identifies the paths for public-private partnership; however, it does not define the mechanism for its implementation. The current *Law on Public-Private Partnership* focuses only on economic partnership and does not serve as an effective mechanism for public-private partnership in the cybersecurity field Assess what budget can be obtained to resource implementation of the strategy and plan cybersecurity measures accordingly. Consider that international donors can be approached to help implement certain measures where national resources are lacking. Commitments concerning budget and necessary human resources are critical for the effective implementation of the strategy and the directive	Establish opportunities and develop mechanisms for public-private partnerships and supporting activities at the regulatory and cybersecurity operational levels
Define targets of awareness-raising campaigns (children, elderly, end-users, C-level executives) Reach out to private sector organizations and international donors to organize and run awareness campaigns on specific cybersecurity topics	Establish a program for digital literacy and cyber hygiene skills development for the public sector and civilian workforce.

Identify gaps of knowledge and expertise in cybersecurity based on the most common cybersecurity incidents	Allow for regular table-top exercises with the participation of key GOU cybersecurity stakeholders, local authorities, and CI operators.
Adoption of a comprehensive law on cybersecurity. Adopted in 2017, the *Law on Cybersecurity* is a roadmap for future regulations. Bearing in mind the Ukrainian legal system and practice, Ukraine would benefit from approving a comprehensive law on cybersecurity in accordance with international standards and best practices that would regulate the full scale of cybersecurity issues. Adoption of such a law requires broad consultations with various stakeholders and the involvement of experts from different fields, including representatives of cybersecurity agencies, in its drafting, to address the complexity of the topic All-inclusive review of the cybersecurity legal framework in compliance with NIS Directive. Ukraine requires a comprehensive review of primary and secondary legislation, identification of norms that contradict the NIS Directive, and proposal of amendments in accordance with the recommendations of the review. Ukrainian authorities lack the capacity to develop relevant drafts of legislation in accordance with NIS Directive requirements and require international assistance Comprehensive review of legislation for consistency of cybersecurity terminology. Different laws regulating cybersecurity were adopted at different times and use different terminology. This significantly complicates the process of their implementation. A comprehensive review of the terminology and harmonization of national legislation is needed to ensure a common understanding of cybersecurity	Develop a new organizational-technical model of cybersecurity governance for Ukraine based on CI risk management principles. Ensure that the terminology used in Ukraine for the cybersecurity sector aligns with international best practices. Adjust existing definitions and introduce new terms common in legislation and European and international standards in this area
Development of strategic internal communication regarding cyber incidents. The NIS Directive requires countries to establish security and communication protocols for operators of essential services and CII/ES. Information sharing about cyber incidents among CI stakeholders and cybersecurity agencies plays an important role in cybersecurity and approval of such requirements contributes to its effectiveness Comprehensive review and amending laws on law enforcement agencies responsible for cybersecurity protection against cybercrimes and cyberterrorism. Ukrainian cybersecurity stakeholders see the role and powers of cybersecurity agencies and the process of assigning such powers differently. Because the *Law on Cybersecurity* assigned significant powers to the SBU and SSSCIP, many representatives of the private sector and NGOs complained that this was done in the *Law on Cybersecurity* instead of amending laws on SBU and SSSCIP. At the same time, the SBU and SSSCIP argue over a lack of powers and resources to work effectively. Ukraine will benefit from careful review and consultations on the delineation of powers between law enforcement agencies responsible for cybersecurity protection.	Develop a new organizational-technical model of cybersecurity governance for Ukraine based on CI risk management principles.

ANNEX 2: LEGISLATIVE ROADMAP

Legislative agenda tasks	Tools	Key stakeholder	Drafted Approved
Develop and approve cybersecurity requirements for CII as baseline security measures and define a series of tiers above that baseline, supported by incentives for exceeding the baseline standards via cyber maturity improvement plans at the organizational level.	*Cybersecurity Law*	VRU	2022 / 2023
Provide sector regulators with the authority to introduce sector-specific standards.			
Develop a common taxonomy for cyber incident classification to be used by CERT-UA, SBU, sector authorities, and CI operators.			
Ensure that the terminology used in Ukraine for the cybersecurity sector aligns with international best practices. Adjust existing definitions and introduce new terms common in legislation and European and international standards in this area.			
Determine the need for support, review, and shaping of the institutional powers of cybersecurity actors; define the principles of cybersecurity governance, ensuring trust and confidence in the interaction between cybersecurity stakeholders, their rights, and responsibilities.			
Identify the role and place of the national regulator(s) of cybersecurity for CI with mandates to coordinate incident response and risk management, while also setting standards for proactive cyber management.			
Define frameworks for self-regulation of private cybersecurity stakeholders and participation in the development of public policy in the field of CI security and resilience			
Define as a good practice to have regular table-top exercises with the participation of key GOU cybersecurity stakeholders, local authorities, and CI operators.			
Define general requirements for conducting a periodic review of the national cybersecurity system governance model, evaluation of its maturity, and implementation of strategic goals			
Define mandatory information security requirements for CII objects, including security risk assessment and business continuity planning requirements, cybersecurity supply chain risk management, etc.;	*Law on Critical Infrastructure Protection*	VRU	2021 / 2021

Legislative agenda tasks	Tools	Key stakeholder	Drafted Approved
Establish legal requirements for CII/ES to manage risks to the security of their systems and facilities; develop business continuity plans; apply monitoring, auditing, and testing of their networks and information systems; and comply with international standards for information or information systems security.			
Clarify the role of SSSCIP regarding the implementation of technical and organizational security measures in public sector CII (e.g., e-governance infrastructure, public registries, etc.).	*Law on SSSCIP*	SSSCIP	2022 / 2023
Review and redefine SSSCIP functions as an actor in the security and defense sector of Ukraine.			
Establish institutional mechanisms for the engagement of key cybersecurity stakeholders in dialogue with CI operators, cybersecurity service providers, the professional cybersecurity community, and experts (including in the form of expert or advisory councils).	*Law on Cyber Public-Private Partnerships*	SSSCIP	2022 / 2023
Ensure the legislative basis for cooperative engagement and mutual capacity building between public and private sector cybersecurity teams including internship, apprenticeship, mentorship programs, etc.	NICE Framework adaptation/localization	SSSCIP	2022 / 2023
Empower industry self-regulation and introduction of certification schemes.	*Law on Cybersecurity Certification Schemes*	SSSCIP	2022 / 2023
Liberalize the market of cybersecurity services, including a shift from licensing for conformity and compliance to a notification procedure for registration as a designated CI entity.	*Law on Cybersecurity Insurance*		2022 / 2023
Define general principles for conducting a review of the national cybersecurity system.	National Cyber Security Strategy	NCCC	2022
Establish requirements for the national CERT-UA and sector CSIRTs.	Regulatory act "Baseline requirements for the national CERT-UA and sector CSIRTs/SOCs"	SSSCIP	2022
Develop a new organizational-technical model of cybersecurity governance for Ukraine based on CI risk management principles.	Regulatory act "On organizational-technical model"	SSSCIP	2022

Legislative agenda tasks	Tools	Key stakeholder	Drafted Approved
Review public procurement legislation to implement Cyber Supply Chain Risk Management requirements.	Regulatory act "On centralized IT procurement"	SSSCIP	2021
Introduce rules and standards overseen by industry regulators.	Regulatory Act "List of rules and standards overseen by industry regulators"	SSSCIP	2023
Implement measures for voluntary vulnerability disclosure in CI sectors, proactive communication regarding current cyber threats, and response and recovery actions, and define the mechanisms for interaction, notification, and the exchange of information inside the cybersecurity ecosystem and with the community at large.	TISM/vulnerability disclosure regulations		2022 / 2023
Develop a cyber workforce development concept.	Resolution CMU on Workforce Plan	NCCC	2022
Establish a program for digital literacy and cyber hygiene skills development for the public sector and civilian workforce. For example, the Activity developed a Cyber Hygiene Program for Chief Digital Transformation Officers, other public servants, and CI operator staff. The Cyber Hygiene Program introduces the basic tenets of cyber hygiene and the role CDTOs play in protecting networks, as well as an overview of modern trends in cybersecurity.	Regulatory Act (State Program)	MDT	2022
Implement risk management requirements in CI sectors based on sector-specific risk.	Resolution "*National CMM Framework*"	SSSCIP	2022
Develop a national response plan for cyber incidents impacting CI with clear protocols for reporting incidents to CERT-UA and sector authorities based on defined severity, including incident management procedures, coordinated actions, and disclosure requirements.	National Response Plan for Cyber Incidents (Regulatory or Approved Decision NCCC)	NCCC/NSDC	2022

ANNEX 3: IDENTIFIED DISCREPANCIES IN TERMINOLOGY

THE DOCUMENT AND THE TERM IN THE EU LEGISLATION	LEGISLATION OF UKRAINE
'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2)	critically important infrastructure objects (hereinafter – objects of critical infrastructure) - enterprises, institutions and organizations, regardless of ownership, whose activities are directly related to technological processes and / or the provision of services of great importance to the economy and industry, functioning of society and security of the population, disabling or disruption of which may have a negative impact on the national security and defense of Ukraine, the environment, cause property damage and / or pose a threat to human life and health
'network and information system' mean: (a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance	information and telecommunication system – a set of information and telecommunication systems that in the process of information processing act as a whole; electronic communications systems (hereinafter referred to as communication systems) – transmission, switching or routing systems, equipment and other resources (including passive network elements that allow the transmission of signals by wired, radio, optical or other electromagnetic means, mobile, satellite network, electrical cable networks in the part in which they are used for the purposes of signal transmission), providing electronic communications (transmission of electronic information resources), including means and devices of communication, computers, other computer equipment, information and telecommunication systems that have access to the Internet and / or other global data transmission networks
'incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto	cyber protection – a set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detection and protection against cyberattacks, elimination of their consequences, restoration of stability and reliability of communication and technological systems
'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems	the term is missing
'national strategy on the security of network and information systems' means a framework providing strategic objectives and priorities on the security of network and information systems at national level	the term is missing
'digital service' means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council which is of a type listed in Annex III 'online marketplace' 'online search engine'	information electronic services – paid or free services for processing and storage of information, provided remotely using information and telecommunication systems at the individual request of their recipient intermediate service in the information sphere – a service for the transmission and / or storage of information and assignment of network identifiers national electronic information resources (hereinafter – national information resources) – systematized electronic information resources that contain information regardless of the type, content, form, time and

THE DOCUMENT AND THE TERM IN THE EU LEGISLATION	LEGISLATION OF UKRAINE
'cloud computing service' 'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (18) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace 'online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found 'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources	place of its creation (including public information, state information resources and other information), designed to meet the vital important social needs of the citizen, the person, a society and the state. Electronic information resources means any information created, recorded, processed or stored in digital or other intangible form by electronic, magnetic, electromagnetic, optical, technical, software or other means
'digital service provider' means any legal person that provides a digital service	"Service Provider" means: i. any public or private institution that provides users of its services with the ability to communicate using a computer system, and ii. any other institution that processes or stores computer data on behalf of such communication service or users of such service. (Convention on Cybercrime Council of Europe; Convention, International Document of 23.11.2001, ratified by the Law of 07.09.2005, №2824-IV)
'incident' means any event having an actual adverse effect on the security of network and information systems	cybersecurity incident – an event or series of adverse events of an unintentional nature (natural, technical, technological, erroneous, including due to human factors) and / or having signs of a possible (potential) cyberattack that pose a security threat electronic communication systems, process control systems, create the possibility of violation of the normal mode of operation of such systems (including disruption and / or blocking of the system, and / or unauthorized management of its resources), endanger the security (protection) of electronic information resources
'cyber space' is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information	cyberspace – an environment (virtual space) that provides opportunities for communication and / or implementation of public relations, formed as a result of the operation of compatible (connected) communication systems and electronic communications using the Internet and / or other global data networks
'cybersecurity' comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats	cybersecurity – protection of vitally important interests of mankind and citizen, society and state during the use of cyberspace, which ensures sustainable development of an information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace

THE DOCUMENT AND THE TERM IN THE EU LEGISLATION	LEGISLATION OF UKRAINE
'information security'. The classic model for information security defines three objectives: Confidentiality, Integrity, and Availability.	technical protection of information – a type of information protection aimed at providing with the help of engineering and technical measures and / or software and hardware means to prevent leakage, destruction and blocking of information, violation of the integrity and availability of information
'network and information security', as defined in ENISA regulation 526/2013, means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the Availability, Authenticity, Integrity and Confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems.	security of networks and services – the ability of electronic communications networks and services to withstand threats to the availability, integrity or confidentiality of those networks and services, data stored, transmitted or processed, and related services provided or accessed through electronic communications networks or services
'cybersecurity' covers all aspects of prevention, forecasting, tolerance, detection, mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security).	cybersecurity – protection of vitally important interests of mankind and citizen, society and state during the use of cyberspace, which ensures sustainable development of an information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace
'cyber ethics'. Ethics are principles and / or standards of human conduct. Cyber ethics is a code of behavior on the Internet. Cyber ethics is the philosophical study of ethics pertaining to computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society.	the term is missing
'cyber hygiene' covers several practices that should be implemented and carried out regularly to protect users and businesses online.	the term is missing
'cyber incident'. Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent of whether it is natural, or human made; malicious or non-malicious intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions it is called a cyber incident. Also, we call cyber incident any incident generated by any of cyber space components even if the damage / disruption, dysfunctionality is caused outside the cyber space.	cybersecurity incident (cyber incident) – an event or series of adverse events of an unintentional nature (natural, technical, technological, erroneous, including due to human factors) and / or having signs of a possible (potential) cyberattack that pose a security threat to electronic communication systems, process control systems, create the possibility of violation of the normal mode of operation of such systems (including disruption and / or blocking of the system, and / or unauthorized management of its resources), endanger the security (protection) of electronic information resources
'cyber accident'. To support a 'grading' of cyber incidents, we define cyber accidents as any occurrence associated with cyber space causing significant damage to cyber space or any other asset (has performance impact, requires repairs, replacement) or causing personal injury.	the term is missing

THE DOCUMENT AND THE TERM IN THE EU LEGISLATION	LEGISLATION OF UKRAINE
'cyber investigation'. A process conducted for the purpose of cyber accident and incident prevention which includes the gathering and analysis of information, the drawing of conclusions, including the determination of causes and, when appropriate, the making of safety and security recommendations	the term is missing
'cyberattacks' cover all cyber incidents triggered by malicious intent where damages, disruptions or dysfunctionalities are caused	cyberattack – directed (deliberate) actions in cyberspace, which are carried out by means of electronic communications (including information and communication technologies, software, software and hardware, other technical and technological means and equipment) and aimed at achieving one or a combination of the following objectives: compromising the confidentiality, integrity, availability of electronic information resources processed (transmitted, stored) in communication and /or technological systems, obtaining unauthorized access to such resources; violation of security, sustainable, reliable and regular operation of communication and /or technological systems; use of the communication system, its resources and means of electronic communications for cyberattacks on other cyber defense objects
'cybercrime' refers to any crime/criminal activity facilitated by or using cyber space	cybercrime (computer crime) – a socially dangerous criminal act in cyber space and / or with its use, liability for which is provided by the law of Ukraine on criminal liability and / or which is recognized as a crime by international treaties of Ukraine
'cyber sabotage' refers to any sabotage activity facilitated by or using cyber space	the term is missing
'cyber espionage': we understand two types of espionage vectors: (a) state espionage (intelligence, when state actors are involved) or (b) industrial espionage (when commercial actors are involved)	the term is missing
'cyber defense' refers to a variety of defensive mechanisms that could be used to mitigate or respond to cyber-attacks	cyber defense – a set of political, economic, social, military, scientific, scientific and technical, informational, legal, organizational and other measures carried out in cyber space and aimed at protecting the sovereignty and defense capabilities of the state, preventing armed conflict and repelling armed aggression
'cyberwarfare' refers to any action by a state, group or criminal organization facilitated by or using cyber space targeting another state	the term is missing
'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions	critical infrastructure – enterprises, institutions and organizations, regardless of ownership, whose activities are directly related to technological processes and / or the provision of services of great importance to the economy and industry, functioning of society and security of the population, disabling or disruption of which may have a negative impact on the national security and defense of Ukraine, the environment, cause property damage and / or pose a threat to human life and health

THE DOCUMENT AND THE TERM IN THE EU LEGISLATION	LEGISLATION OF UKRAINE
'risk analysis' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure	the term is missing
'sensitive critical infrastructure protection related information' means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations	the term is missing
'owners/operators of ECIs' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive	electronic communications operator (operator) – an economic entity that owns, operates and manages electronic communications networks and / or related facilities.

ANNEX 4: REFERENCES

An Evaluation Framework for Cyber Security Strategies
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

Blueprint Energy Solutions GmbH. Final Report – Study on Cyber Security in the Energy Sector of the Energy Community. 2019
https://drive.google.com/file/d/1ZJxVUgSrxHMQAzuMLXuCcQhy6VEkdhPd/ view?usp=sharing

Decree of the President of Ukraine of July 29, 2019, № 558/2019 -
https://zakon.rada.gov.ua/laws/show/ 558/2019#n16

EU Support to Cybersecurity in Ukraine Project. Final Draft Report. 2018 -
https://drive.google.com/file/d/1eO61HrrPurqznHVP_4iu48uh4ZJWKilY/view?usp=sharing

First National Cyber Security Strategy Good Practice Guide
https://www.enisa.europa.eu/publications/ncss-good-practice-guide;

Good practices in innovation on Cybersecurity under the NCSS
https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1;

International Foundation for Electoral Systems. Ukrainian Cybersecurity Legal Framework: Overview and Analysis. 2019 https://drive.google.com/file/d/1PZOvvGCLVMnaPPOwr03IxQYVm-w95KAv/view?usp=sharing

Law of Ukraine "On Basic Principles of Cybersecurity of Ukraine" https://zakon.rada.gov.ua/laws/show/2163-19

MITRE. Stakeholder Re-calibration and Election Security Engagements After-Action Report and Recommendations. 2018 https://drive.google.com/file/d/1oFX6VnAn4PYq0Jf9wKuG-3SEu_sFMrly/view?usp=sharing

National Coordination Center for Cyber Security on NSDC website
https://www.rnbo.gov.ua/ua/Diialnist/4658.html

National Cyber Security Strategies – Interactive Map https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map;

National Cyber Security Strategies (NCSS): An Implementation Guide
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide;

National Cybersecurity Strategies Evaluation Tool https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool;

National Cybersecurity Strategies Training Tool https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/ncss-training-tool

Order of the Cabinet of Ministers of Ukraine "*On Approval of the Concept of Creating a State System for Critical Infrastructure Protection*" https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80

Resolution of the Cabinet of Ministers of Ukraine "*On Approval of the General Requirements for Cyber Protection of Critical Infrastructure Objects*" https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF

Resolution of the Cabinet of Ministers of Ukraine "*On approval of the List of State-owned Objects of Strategic Importance for the Economy and Security of the State*" https://zakon.rada.gov.ua/laws/show/83-2015-%D0%BF