NCSCC
NATIONAL CYBERSECURITY COORDINATION CENTER

USAID
FROM THE AMERICAN PEOPLE

ICWR
STITUTE OF CYBER WARFARE RESEARCH

ASSESSMENT OF NATIONAL CYBER CAPABILITIES:

WHAT IS THE LEVEL OF CYBERSECURITY MATURITY OF UKRAINE ACCORDING TO THE ENISA METHODOLOGY?

The study "Assessment of National Cyber Capabilities: What is the Level of Cybersecurity Maturity of Ukraine According to the ENISA Methodology?" was made possible through support provided by the U.S. Agency for International Development within the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Governmen.

NCSCC
NATIONAL CYBERSECURITY COORDINATION CENTER

USAID
FROM THE AMERICAN PEOPLE

ICWR
INSTITUTE OF CYBER WARFARE RESEARCH

CONTENT

INTRODUCTION

The cyber aspect continues to be an important element of Russia's hybrid efforts to complement its military actions against Ukraine.

Thus, Ukraine, with significant assistance from international partners, is actively reforming its cybersecurity system, enhancing its technical and human resources, exchanging information with partners and implementing international standards and approaches.

The final point is especially important considering Ukraine's clear European integration course and, therefore, the need to converge approaches with European partners in terms of principals of state policy formation, policy priorities and technical capacity development.

On November 13, 2023, Ukraine and the European Union Agency for Cybersecurity (ENISA) signed a Working Agreement aimed at raising awareness of parties to strengthen cyber resilience, sharing best practices to ensure harmonization of laws and implementation, and exchanging knowledge and information on the cybersecurity threat landscape.

ENISA is the key EU agency that provides methodological assistance to all countries in development of cybersecurity, facilitates information and best practices exchange, and creates a common space of cybersecurity guidelines for all European countries to make them more resilient to cyberthreats.

Ukraine needs to become a part of the European cybersecurity space, as well as to be a part of the European cyber family. This is impossible without close cooperation with European institutions and a common understanding of the cyberthreat landscape and the cyber potential of European countries. However, without a quantitative measurement of this potential and a clear understanding of the level of implementation of cybersecurity practices, it is difficult to understand the trajectory of movement towards better cyber resilience.

In 2020, ENISA tried to solve this problem by offering all countries its own methodology for measuring cyber maturity – the National Capabilities Assessment Framework. The document provides specific recommendations and guidelines for countries to assess how well they have implemented best practices and key policies on the way to cybersecurity development. This study aims to initiate a process of assessing Ukraine's national cyber maturity level to aid our country to become a part of the EU's common cybersecurity space.

This is the first attempt, which should not only provide relevant results based on ENISA approaches, but also assists to understand limits of this assessment model and suggests possible refinements to the use of the methodology and a procedure of conducting the assessment in future.

The cyber maturity assessment is not only an important element of assessing the current state of national cybersecurity, but also a set of valuable data ahead of updating the key strategic document – the Cybersecurity Strategy of Ukraine. This is an opportunity to take a critical look at current achievements and understand what ideas and tasks need to be included in the updated strategic document.

This definition of the level of cyber maturity is also an opportunity to additionally assess an effectiveness of a gradual implementation of the Strategy in a long term.

METHODOLOGY AND DESIGN OF THE RESEARCH

This study is based on an adapted version of the ENISA National Capabilities Assessment Framework methodology[1], which contains key approaches to conducting a comprehensive assessment of the EU countries in terms of their cybersecurity maturity.

This assessment is conducted in two main directions: assessment of maturity of the strategic approach to cybersecurity (in fact, an existence of strategic documents and certain national policies/ practices) and assessment of cybersecurity capability maturity, which aims to determine the country's real cyber potential in 17 different fields (goals). These goals include:

- ✓ development of the National Cyber Security Incident Response Plan(s);
- ✓ establishment of basic security measures;
- ✓ ensuring protection of digital identification and building trust in digital state services;
- ✓ establishment of digital response capabilities;
- ✓ raising users' awareness;
- ✓ organization of cybersecurity training;
- ✓ improving training and educational programs;
- ✓ facilitating scientific research and development work;
- ✓ encouraging private sector to invest in security measures;
- ✓ strengthening of supply chain cybersecurity;
- ✓ protection of critical informational infrastructure (CII), basic service operators and digital service providers;
- ✓ counteraction to cybercrime;
- ✓ establishment of incident report mechanism;
- ✓ strengthening data privacy protection;
- ✓ establishment of public-private partnership (PPP);
- ✓ institutionalizing cooperation among state agencies;
- ✓ engaging in international cooperation (not only with the EU member countries).

The assessment of maturity of strategic approach to cybersecurity is determined through a set of identical, repeated questions for each block (questions in blocks a, b and c).

To assess maturity of cyber capability, questions from 1 to 13 are used (different numbers of questions for different purposes to determine the level of maturity). In total, this block contains 319 questions.

Both blocks contain «mandatory» questions (marked with «1» in column R) and «secondary» questions (not critical to confirm the level of cybersecurity maturity, marked with «0» in column R). All questions have only «Yes» or «No» answers.

1 https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

The general requirement for determining any of the above maturity levels is consistency. In this approach, to move to the next level of cybersecurity maturity, requirements of a particular maturity level must be fully met (positive answers to all «mandatory» questions). Accordingly, it is not possible to move to the next level if all the tasks of the previous one have not been completed.

The ENISA methodology also proposes to additionally determine a scale of coverage of national efforts for each goal – in fact, it is an assessment of country's overall efforts within a particular goal, where these efforts may be more significant than a formal determination of the level of cybersecurity maturity.

Although the basic methodology provides for a possibility of changing the number of goals to be assessed, as well as some adjustment of the methodology (to better adjust to a situation of each country), this study choses an approach of following basic guidelines as closely as possible to create an indicator that is as close as possible to the logic of information to methodological requirements of ENISA.

The Fieldwork was conducted between February and March 2024 and included preparation of questionaries in accordance with the ENISA guidelines, sending them to respondents and processing the results. In addition, between April and May 2024, experts worked on certain indicators of the questionnaire and made some adjustments to final answers (for example, the fact of creation of an Interagency Working Group on Attracting International Assistance to ensure cybersecurity and cyber resilience of the state was not indicated in basic questionnaires).

In total, the research surveyed 40 organizations, including all members of the National Security Coordination Center, 10 Central Executive Authorities, 20 reginal state administrations, 2 scientific institutions and 1 private company providing cybersecurity services.

GENERAL CONCLUSIONS OF THE RESEARCH

☑ The current regulatory framework (primarily – the Cybersecurity Strategy of Ukraine and annual plans for its implementation) **almost corresponds to the third level**.

☑ The most notable achievements (level 5 of maturity of the strategic approach) are:

- national cybersecurity incident response plans;
- scientific research and development activities;
- protection of critical information infrastructure;
- counteracting cybercrime.

☑ The respondents also identified the strategic approach to the development of public-private partnership in Ukraine as Level 5. At the same time, only the objectives of the Cybersecurity Strategy of Ukraine and an annual plan for its implementation are referred to as confirming indicators. In future assessments, this issue will be subject to a more balanced assessment to clarify key achievements in this field.

☑ Strategically, the most difficult situation is in 3 fields (in each of these fields the level of policy maturity does not exceed one):

- encourage the private sector to invest in security measures;
- supply chain cybersecurity;
- data privacy protection.

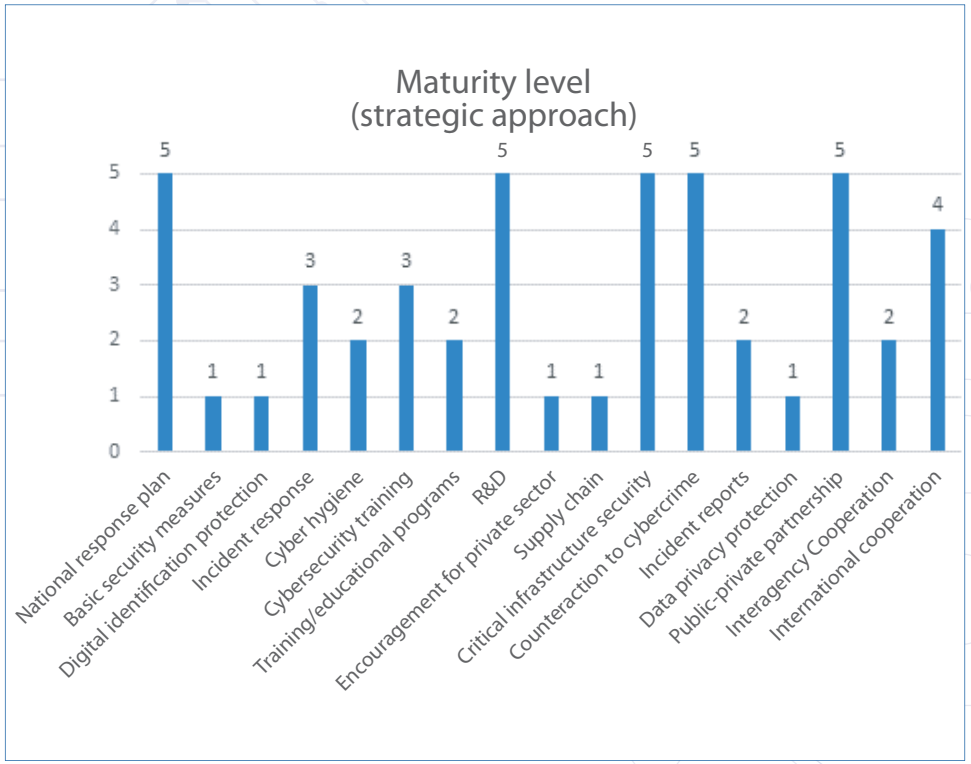
☑ Supply chain security is the least implemented goal. Here, not only the maturity level of the strategic approach equals to one, but Ukraine has not even managed to reach the first level of cybersecurity maturity in terms of cyber capabilities: even the first basic task has not been completed.

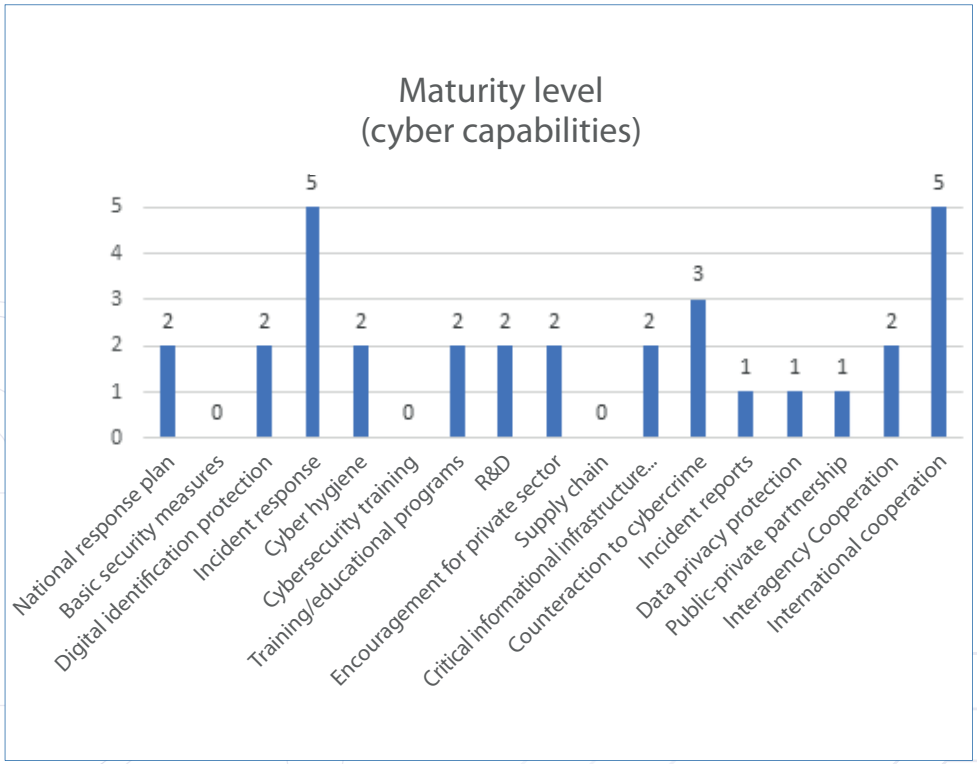
☑ Although **an average maturity level of cyber capabilities almost corresponds to maturity level 2**, this indicator does not fully reflect the government's actual efforts. The last one is represented by the indicator «coverage scale» – a percentage of positive answers to questions in a table related to a total number of questions. There are 3 groups, that are exemplary in this regard:

establishing basic security measures. In terms of formality, the maturity level of cyber capabilities here is zero: two basic tasks have not been completed. However, the coverage for this goal is 74%. The state has fulfilled many tasks that correspond to levels 4 and even 5 of cybersecurity maturity;

organization of cybersecurity training. Due to a failure to implement one of two tasks of the first maturity level, Ukraine failed to reach even the first level of cybersecurity maturity. However, the coverage scale here is 68% (most tasks for levels 3 and 4 of cybersecurity maturity have been completed);

institutional cooperation among state agencies. According to this indicator, the maturity level of cyber capabilities is 2. However, the coverage scale is 90%. Respondents negatively assessed only 1 step of tasks of this goal, which is mandatory for obtaining the level 3 of maturity.





☑ In general, the largest number of negative responses was related to an absence of tools (for different purposes) to evaluate effectiveness of measures implemented and, consequently, to adjust them. In fact, the Ukrainian approach to planning is mostly goal-oriented but does not provide flexibility in adjusting the approach or evaluation its effectiveness.

☑ Some goals are not entirely relevant to the Ukrainian conditions (which lowered the score) but are important in terms of understanding development priorities. For example, in several strategic goals, one of the indicators is a formalized interaction with pan-European institutions. Ukraine, which is not a member of the EU, cannot fulfill these requirements. However, these steps indicate European formats that Ukraine should join in the near future.

	Maturity level (strategic approach)	Maturity level (cyber capa-bilities)	Coverage scale (in percentage)	Name of the goal
1	5	2	87%	development of the National Cyber Security Incident Response Plan(s)
2	1	0	74%	establishing basic security measures
3	1	2	88%	ensuring protection of digital identification and building trust in digital state services
4	3	5	100%	establishment of digital response capabilities
5	2	2	53%	raising user' awareness
6	3	0	68%	organization of cybersecurity training
7	2	2	76%	improving training and educational programs
8	5	2	83%	facilitating scientific research and development work
9	1	2	36%	encouraging private sector to invest in security measures
10	1	0	13%	strengthening of supply chain cybersecurity
11	5	2	67%	protection of critical informational infrastructure (CII), basic service operators and digital service providers
12	5	3	95%	counteraction to cybercrime
13	2	1	67%	establishment of incident report mechanism
14	1	1	25%	strengthening data privacy protection
15	5	1	56%	establishment of public-private partnership (PPP)
16	2	2	90%	institutionalizing cooperation among state agencies
17	4	5	100%	engaging in international cooperation (not only with the EU member countries)

☑ Ukraine has a number of achievements and existing cyberliteracy programs. At the same time, as an analysis of questions and answers regarding Goal 5 shows, Ukrainian policy lacks institutionalizations and consistency in this area. One-off events or creation of content that is not integrated into a broader digital awareness strategy and an absence of measures to review these communication activities have lowered Ukraine's position in terms of maturity according to this step.

☑ The situation is similar with Goal 6 – cybersecurity training. In recent years, such trainings have been conducted more and more often, but the factor that has lowered Ukraine's performance here is an absence of consistency in this process, as well as established and understandable practice of «lessons learned» (implementation of new developments after trainings or analysis of crisis situations).

☑ There are significant problems with Goal 9 – private sector encouragement. The EU has a traditional approach where the private sector is actively involved in cybersecurity activities through a clear system of rewards and compensations (the similar approach is adopted in the EU Cyber Solidarity Act). At the same time, this approach relies on available pan-European resources, relevant practice and mostly peaceful progressive development of the EU. Under conditions of war, a severe lack of financial and human resources, Ukraine's ability to stimulate the private sector in these matters is quite limited. Perhaps, in its current form, this Goal cannot be fully applied to Ukraine (at least at this stage) or should be transformed to consider an objective military and political situation in the country.

☑ The problem with supply chain cybersecurity (Goal 10) was already mentioned at the beginning of the conclusions. This issue lacks both the coherent state policy and methodological materials. This is an issue where Ukraine will need the most efforts, especially paying attention to growing threats to critical infrastructure attacks of this type.

☑ Although Ukraine's overall success in implementing Goal 11 (critical infrastructure (CI) security) is quite successful, respondents point to a problem of mapping CI threats, am absence of the national risk register and a lack of understanding of CI correlations (both at national and international levels). At the same time, these fields of activity are understandable and can be corrected quite quickly.

☑ Personal data protection (Goal 14) is also one of the important future focuses for increasing the level of cybersecurity maturity. Despite well-developed legislation on personal data protection, the cybersecurity aspect of this protection, reporting on cyber incidents that resulted in personal data leaks, spreading information on best practices in personal data protection among various target groups, this all still requires special attention from government.

☑ Although the public-private partnership (Goal 15) is an element of ongoing discussion in an expert community, institutionalization and definition of specific forms of such cooperation in Ukraine is still difficult. Only the first level of cybersecurity maturity in terms of capabilities indicates that many important elements have not yet been implemented: there is no agency that coordinates the public-private partnership in cyberspace, no national plan for development of this field, no funding for such cooperation in organization's budgets, etc.

☑ A situation with cooperation among state agencies is positive (Goal 16). The only noticeable problem is an absence of interaction and cooperation among cyber specialists at a regional level: there are no permanent (or at least regular) interaction formats for them to share experience and best practices.

☑ International cooperation (Goal 17) is probably the most dynamic and comprehensive as of today. The only warning from the experts was an absence of a mechanism to ensure dynamic adaptation of the action plan regarding this Goal in accordance with changes in the environment. Even though the absence of this mechanism was noted, it should be mentioned that the mechanism could be a format of both bilateral and multilateral dialogues, the agenda of which is formed in accordance with current needs of Ukraine. Another such mechanism could be the Tallin Mechanism.

ORGANIZATIONAL CONCLUSIONS

While the main purpose of the research was to determine the level of cybersecurity maturity of Ukraine, a process of questioning, collecting results and analyzing the research allows us to draw a number of conclusions about process itself and will be useful for future research using this methodology. These conclusions include:

☑ There are noticeable differences in a quality of filling out the questionaries. The main entities of the national cybersecurity system mostly filled out the questionaries responsibly (adding supporting comments or references where possible), while local authorities, scientific organizations and non-core Central Executive Authorities filled out the questionaries either partially (many fields were left blank) or did not provide supporting details.

☑ For future assessments, it is obvious that there is a need to add another field to each question with a brief explanation of its meaning. It is noticeable that in many cases the respondents answered questions according to their perspective of a situation in their organization, rather than in a national context. The situation was particularly complicated with the questions of strategic approach assessment block. The basic methodology provided for a wide range of questions that allowed for a flexible description of the country's real achievements on this path. However, this approach is not very successful for highly normative Ukrainian practice.

☑ The absence of supporting positions in many questions greatly complicates the analysis of real achievements. In a complete absence of supporting positions for some questions, the authors of this research proceeded from a position of prevailing most answers to a particular question («Yes» or «No»), which is a certain assumption from the point of view of assessing the real result.

☑ An absolutely anonymous survey is not effective enough for such research. The basic hypothesis of the research assumed that the survey of a sufficient number of experts involved in the issue with an opportunity to provide them with necessary comments on their answers (with a strict model of the main answer in a dichotomy «Yes» or «No») would allow collecting appropriate empirical material. A large number of unconfirmed responses indicates the need to supplement the questionnaire with in-depth interviews of strategic sessions with representatives of the NCCC members to form initial assessments, references to supporting documents of an ability to record respondents' assessments that cannot be confirmed by relevant documents or references.

☑ The methodology needs to be improved and adjusted. Although the research is based on the ENISA's core questions as close as possible (with minor adjustments to reflect national peculiarities), some of the questions in the questionnaire are not relevant to the current situation. For example, the question about a degree of implementation of the NIS Directive. Ukraine did not have such obligations in the past but is currently preparing to implement the NIS2 Directive. Such matters need to be significantly updated.

APPENDIXES

Goal 1 – to develop National Cybersecurity Incident Response Plans

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan regarding the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are there expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Has work on developing national cybersecurity incident response plans begun? For example, setting out general objectives, scope and/ or principles of incident response plans, etc.	1	Is there a doctrine/ national strategy that includes cybersecurity as a crisis factor (i.e., project, policy, etc.)?	1	Is there a cyber crisis management plan at the national level?	1	Are you satisfied with a number or percentage of critical sectors included in the national cybersecurity incident response plan?	1	Is there a procedure for learning from lessons learned after cybersecurity training or real crises at the national level?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2	Is it cowell known that cyber incidents are a crisis factor that can threaten national security?	0	Is there a center for obtaining information and informing decision makers? That are, any methods, platforms, or locations to ensure that all crisis response participants have an access to the same information about the cyber crisis in real time.	1	Are there procedures at the national level to deal with cyber crises?	1	Are activities (i.e., trainings) related to the national cybersecurity incident response plans organized frequently enough?	1	Is there a process for regular testing of the national plan?	1
3	Have studies (technical, operational, organizational and managerial) been conducted in the field of the cybersecurity incident response plans?	0	Are there appropriate resources to supervise a development and implementation of national cybersecurity incident response plans?	1	Is there a communication team in your organization specifically trained to respond to cyber crises and inform the public?	1	Are there enough people in your organization to plan for crises, learn from lessons learned, and implement changes?	1	Are there proper tools and platforms for creating situational awareness?	1
4			Is there a cyber threat assessment methodology at the national level that includes an impact of assessment procedures?	0	Are all relevant national agencies involved (security and defense agencies, civil protection, law enforcement, state agencies, etc.)?	1	Are there enough people in your organization trained to respond to cyber crises at the national level?	1	Do you follow the specific maturity model to monitor and improve your cybersecurity incident response plans?	0

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
5					Do you have appropriate crises management tools and situational rooms?	1			Do you have resources that specialize in either threat prevention or forecasting cybersecurity to address future crises or tomorrow's challenges?	0
6					Do you interact with the EU international interested parties when necessary?	0				
7					If necessary, do you interact with international interested parties from the non-EU countries?	0				

Recommendations

- ✓ a work on preparation and approval of the National Cyber Incident Response Plan should be completed (a necessary condition for moving to the maturity level 3);
- ✓ this plan should be subjected to regular testing during national tabletop exercises (the condition for reaching the maturity level 5);
- ✓ it is also advisable to work with the ENISA partners to develop possible maturity levels for the plan.

Goal 2 – to establish basic security measures

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan regarding the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Have research been conducted to identify requirements and gaps for public organizations based on internationally recognized standards? For example, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS etc.	1	Are security measures adopted (at a country level) in accordance with international/national standards?	1	Are basic security measures mandatory?	1	Is there a process for periodically updating basic security measures?	1	Are there mechanisms to improve Informational Technological Support protection when basic security measures fail to respond and resolve incidents?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2	Has research been conducted to identify requirements and gaps for private organizations based on internationally recognized standards? For example, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS, etc.	1	Is a consultation provided for the private sector and other relevant agencies when defining basic security measures?	1	Are horizontal security measures applied in critical sectors?	1	Is a monitoring mechanism implemented to review an adoption of basic security measures?	1	Are new standards developed in response to recent changes in the threat environment assessed for compliance?	1
3					Are sectoral security measures applied in critical sectors?	1	Is there a national agency that verifies an implementation of basic security measures?	1	Do you have or promote the national coordinated vulnerability disclosure (CVD) process?	1
4					Do basic security measures comply with the applied certification schemes?	1	Is there a process established for identifying non-compliant organizations over a period of time?	1		
5					Is a risk self-assessment process implemented for basic security measures?	1	Is there an audit process for ensuring security measures to be properly implemented?	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
6					Are mandatory basic security measures analyzed in a procurement process by state agencies?	0	Are security standards approved for development of critical software and hardware (medical equipment, networked and autonomous vehicles, radio communications, industrial equipment, etc.)?	0		

Recommendations

✓ determining basic cybersecurity measures remains an important element in achieving a high level of cybersecurity maturity (reaching level 1);

✓ according to a decision of the NCCC it is advisable to initiate expert research to determine general requirements and gaps of cybersecurity, that are typical for public-private organizations (for example, based on international standards: ISO27001, ISO27002, BS 15000, PCI-DSS, CobiT, NIST, IEC, CIS etc. (this measure is a necessary condition for achieving cybersecurity the maturity level 1));

✓ based on the NCCC to create a working group with representatives of main agencies of national cybersecurity system, as well as interested stakeholders regarding development of approaches to determine basic cybersecurity requirements (reaching level 2);

✓ to consider a possibility of establishing a necessity for compliance with basic cybersecurity requirements by all participants who provide their services to the state sector in the procurement process. Annually assess compliance with these requirements, in particular through a mandatory self-assessment mechanism for such suppliers (an additional condition for achieving level 3);

✓ to conduct random inspections of such organizations to ensure that they actually comply with basic cybersecurity requirements;

✓ to carry out an annual assessment of the compliance of new cybersecurity standards (developed during the last calendar year) with the current cyber threat landscape of Ukraine (general assessment of whether the implementation of each of new standards will assist to respond to a specific threat from the threat landscape) – (achievement of level 5)).

Goal 3 – to ensure protection of digital identification and build trust to digital state services

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Have studies or gap analyses been conducted to determine needs for protection of digital state services for citizens and businesses?	1	Is a risk analysis performed to determine the risk profile of assets or services before moving them to the cloud or engaging in any digital tran sformation projects?	1	Is there any support for implementation of methodologies with a built-in privacy algorithm in all e-government projects?	1	Is data collected on cybersecurity incidents involving a failure of digital state services?	1	Does Ukraine (or your organization) participate in international working groups to maintain standards and/or develop new requirements for electronic trust services (electronic signatures,	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
1									electronic seals, registered electronic delivery, time stamping, website authentication)? For example, ETSI/CEN/ CENELEC, ISO, IETF, NIST, ITU etc.	1
2			Is there a strategy for building or promoting secure national electronic identification (eID) schemes for citizens and businesses?	1	Are private stakeholders involved in development and delivery of secure digital public services?	1	Has mutual recognition of electronic identification devices been implemented with the EU member countries?	1	Does Ukraine (or your organization) participate in a preparation of peer reviews of electronic identification (eID) schemes?	1
3			Is there a strategy for building or promoting an implementation of secure national electronic trust services (electronic signatures, electronic seals, registered electronic delivery, time stamping, website authentication) for citizens and businesses?	1	Is the minimum basic level of security implemented for all digital state services?	1				

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
4			Is there a strategy for e-government clouds (a cloud strategy for the government and state agencies, such as ministries, government departments and state administrations, etc.) that takes into account security implications?	0	Are any electronic identification schemes available for citizens and businesses with a significant or high level of security, as defined in the Appendix to the Regulation (EU) No. 910/2014 eIDAS?	1				
5					Does any digital state services that require electronic identification schemes with a significant or high level of security exist, as defined in the Appendix to the Regulation (EU) No. 910/2014 eIDAS?	1				
6					Do providers of trust services for citizens and businesses exist (electronic signatures, electronic seals, registered electronic delivery, time stamping, website authentication)?	1				

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
7					Are you aware of programs that promote an adoption of basic security measures for all cloud deployment models (e.g., Private, Public, Hybrid, IaaS, PaaS, SaaS)?	0				

Recommendations

✓ to establish a permanent working group to form offers regarding improvement of a condition of digital identification protection and strengthening of trust in digital state services (level 2);

✓ to define at the level of Resolution / Order of the Cabinet of Ministers of Ukraine a necessity to implement approaches with a built-in privacy algorithm in all e-government / digital transformation projects (level 4);

✓ The Ministry of Digital Transformation of Ukraine should consider starting a dialogue with the European partners on involving Ukraine in conducting peer reviews of electronic identification (eID) schemes (level 5).

Goal 4 – to establish incident response capabilities

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Do informal incident response capabilities that are managed by the state or the private sector, exist or are they mutually managed?	1	Is there at least one official national CSIRT team?	1	Does an incident response capability exist for the sectors defined in Appendix II of the NIS Directive?	1	Have standardized practices been defined/ implemented for incident response procedures and incident classification schemes?	1	Are there mechanisms for early detection, identification, prevention, response and consequences reduction of zero-day vulnerabilities?	1
2			Do national the CSIRT teams have a clearly defined scope of intervention? For example, depending on the target sector, types of incidents, consequences.	1	Does Ukraine have a mechanism for cooperation of the CSIRT team to respond to incidents?	1	Is the incident response capability assessed to ensure that you have sufficient resources and skills to fulfill the tasks as defined in step (2) of Appendix I of the NIS Directive?	1		
3			Do national the CSIRT teams have a clearly defined framework for dealing with other national interested parties regarding the national cybersecurity	0	Are national the CSIRT teams capable of responding to an incident in accordance with Appendix I of the NIS Directive? That is, availability, physical	1				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
3			environment and incident response practices (e.g., law enforcement agencies, military, internet service providers, national cybersecurity center)?	0	security, business continuity, international cooperation, incident monitoring, early warning and notification capability, incident response, risk analysis and situational awareness, cooperation with the private sector, standard operating procedures, etc.	1				
4					Does a mechanism exist to cooperate with other neighboring countries on incidents?	1				
5					Are clear incident handling policies and procedures formalized?	1				
6					Do national the CSIRT teams participate in cybersecurity training both nationally and internationally?	1				
7					Is the national CSIRT team involved in the FIRST (Forum of Incident Response and Security Teams)?	0				

Recommendations

✓ by a decision of the NCCC to oblige cybersecurity entities to assess compliance of all cyber incident response protocols at least once a year, as well as to check their effectiveness and functionality (level 5).

Goal 5 – to raise users' awareness

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Is there minimal recognition by the government, the private sector, or general users that there is a need to raise awareness of cybersecurity and privacy issues?	1	Has a specific target audience been identified for user awareness? For example, general users, young people, business users (small and mid-sized businesses, basic service operators, digital service providers, etc.).	1	Have communication plans/strategies been developed for the campaigns?	1	Have metrics been developed to evaluate the national campaign at the planning stage?	1	Are mechanisms implemented to ensure that awareness-raising campaigns remain relevant to technological advances, changes in the threat environment, legal regulations, and national security directives?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2	Do state agencies conduct cybersecurity awareness campaigns within their organization when necessary? For example, after a cybersecurity incident.	0	Is the action plan prepared to raise awareness of information security and data privacy issues?	1	Is there a process for creating content aimed at improving cyber hygiene at the state level?	1	Is the incident response capability assessed to ensure that you have sufficient resources and skills to fulfill the tasks as defined in step (2) of Appendix I of the NIS Directive?	1	Are campaigns evaluated after they are completed?	1
3	Do state agencies conduct cybersecurity awareness campaigns for the general public when necessary? For example, after a cybersecurity incident..	0	Does the state have accessible and easily recognizable resources (e.g., a single online portal, a set of awareness-raising tools) for users seeking to learn about cybersecurity and privacy issues?	1	Do mechanisms exist for identifying those target groups that require priority cyber awareness (e.g., ENISA Threat Environment Assessment, reports from national cybercrime centers, etc.)?	1	Are there any mechanisms implemented to determine the most appropriate media or communication channels depending on the target audience to maximize outreach and engagement? For example, different types of digital media, brochures, emails, educational material, posters in public places, television, radio, etc.	1	Are consultations held with behavioral experts to adapt the communication campaign to the target audience?	1
4					Is there a practice of bringing together interested parties with experts and communications teams to create content?	1				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
5					Is the private sector involved in information campaigns and spreading messages to a wider audience?	1				
6					Are there any specific awareness-raising initiatives prepared for leaders in the state, private, academic, or civil society sectors?	1				
7					Are there any events held as part of the annual cybersecurity months?	0				

Recommendations

✓ those responsible for the thematic points of the Cybersecurity Strategy should form a working group to develop the National Program for raising cyber awareness / cyber education (it is recommended to use the materials of the AR-in-the-box ENISA during its development);

✓ to provide that the National Program should contain the following: metrics for its implementation, a procedure for regular (at least once a year) assessment of the effectiveness of its implementation, clearly defined and prioritized target groups for raising cyber awareness (the last ones should be reviewed throughout an implementation of the entire National Program based on assessments of the cyber threat landscape), and the main channels of communication for a formation of cyber awareness;

✓ the National Program should contain a constantly (once a year) updated communication plan: the main ideas of the information campaign, ways of their implementation and expected coverage indicators;

✓ after development and approval of the National Program, it is advisable to establish a permanent group of representatives of state agencies, communication experts (with mandatory inclusion of behavioral experts) and the private sector under the main agency responsible for its implementation to constantly assess the effectiveness of the National Program and provide proposals for its optimization.

Goal 6 – to organize cybersecurity trainings

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Are crisis training exercises conducted in other sectors (other than cybersecurity) at the national level?	1	Is there a cybersecurity training program at the national level?	1	Are all relevant state agencies involved (even if the scenario is specific to a particular sector)?	1	Are there post activity reports/evaluation reports prepared?	1	Is there a capability to analyze an experience gained in the cyber field (reporting processes, analysis, consequence reduction)?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2	Are resources allocated to developing and planning crisis management training?	1	Are cyber crisis management exercises conducted for vital social functions and critical infrastructure?	1	Is the private sector involved in planning and performance of trainings?	1	Are national-level plans and procedures reviewed?	1	Is there an organized process for lessons learned?	1
3			Has a coordinating agency been identified to monitor the development and planning of cybersecurity trainings (state agency, consultancy, etc.)?	0	Are sector-specific trainings organized at the national and/or international level?	1	Do Ukrainian representatives participate in cybersecurity trainings at the European level?	1	Is the training scenario adapted to the latest developments (technological advances, global conflicts, threat environment, etc.)?	1
4					Is there a practice of organizing trainings in all critical sectors as defined in Appendix II of the NIS Directive?	1			Are crisis management procedures coordinated with international partners to ensure an effective national crisis management?	1
5					Are there any cross-sectoral cybersecurity trainings?	1			Is there an implemented mechanism to quickly adapt strategies, plans, and procedures based on lessons learned after trainings?	0
6					Is cybersecurity training specific to different levels (technical and operational level, procedure level, decision-making level, political level, etc.)?	0				

Recommendations

✓ entities implementing the Cybersecurity Strategy, when submitting suggestions to the annual plans for implementation of the Cybersecurity Strategy, to include expenses for conducting training exercises with personnel in terms of crisis response and management (level 1);

✓ the National Plan of Protection and Ensuring the Security and Resilience of Critical Infrastructure should provide for mandatory trainings on crisis response and management in all sectors of critical infrastructure, as specified in the Law of Ukraine "On Critical Infrastructure" and the Resolution of the Cabinet of Ministers of Ukraine of October 9, 2020 No. 1109 (level 3);

✓ The NCCC, together with the State Service of Special Communications and Information Protection of Ukraine, to develop a generalized plan for cybersecurity trainings and to review it periodically for compliance with the current needs of the state in such trainings;

✓ to establish an obligation for all major entities of the national cybersecurity system and CI operators to participate in at least one national-level tabletop exercises (hybrid threats and/or sectoral threats);

✓ to ensure in the National Cyber Incident Response Plan an obligation of attacked organizations and key entities of the national cybersecurity system to conduct the «lessons learned» procedure, and for the State Service of Special Communications and Information Protection of Ukraine, together with the Security Service of Ukraine and the NCCC, to develop a standard methodology for this procedure. Determine an obligation to make changes to object-based cyber incident response plans based on «lessons learned»;

✓ to conduct series of consultations with international partners (for example, in a format of bilateral dialogues or in accordance with international cooperation agreements signed by Ukraine) to coordinate joint response to cross-border incidents.

Goal 7 – to improve training and educational programs

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan regarding the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Do state agencies consider developing training and educational programs on cybersecurity?	1	Are cybersecurity courses established?	1	Is cybersecurity culture integrated into early stages of an ducational process in Ukraine? For example, are cybersecurity courses introduced in middle schools and high schools?	1	Does the government encourage employees in the public-private sectors to become accredited or certified professionals?	1	Are there implemented mechanisms to ensure that training and educational programs are kept up-to-date with current and emerging technological developments, changes in the threat environment, legal regulations and national security directives?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2			Do Ukrainian universities offer PhD programs in cybersecurity as an independent discipline rather than as a branch of Information Technology?	1	Are there any national research laboratories and educational institutions in Ukraine that specialize in cybersecurity?	1	Has Ukraine developed cybersecurity training or mentoring programs to support national startups and small and mid-sized businesses?	1	Are academic centers of advanced training in cybersecurity being established as centers of research and education?	1
3			Are there plans to train educators (regardless of their field) on information security and data privacy? For example, Internet safety, personal data protection, cyberbullying.	1	Are special cybersecurity courses and retraining curricula encouraged/ funded at employment centers?	1	Is there a practice of actively promoting information security courses in higher education programs not only for students studying computer science, but also for any other profession or specialty? For example, courses tailored to the needs of a particular profession.	1	Do academic institutions participate in leading discussions on cybersecurity education and research at the international level?	0
4					Are there courses and/ or specialized programs in cybersecurity for EQF (European Qualification Framework) levels 5-8?	1	Is there a regular assessment of a lack of professional training (shortage of employees) in the field of cybersecurity?	1		
5					Does the state encourage initiatives to include Internet safety courses in primary and secondary education?	1	Is there a practice of promoting development of networks and information exchange among scientific institutions at both the national and international levels?	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
6					Is there a practice of funding or free basic cybersecurity training for citizens?	0	Is the private sector involved in any way in cybersecurity education initiatives? For example, in development and delivery of courses, internships, employment, etc.	1		
7					Are there annual cybersecurity events organized (e.g., hacker competitions or hackathons)?	0	Are there funding mechanisms implemented to encourage a pursuit of cybersecurity education/ science degrees? For example, scholarships, guaranteed internships/ practices, guaranteed jobs in a specific industry or in public sector positions.	0		

Recommendations

✓ although the Cybersecurity Strategy of Ukraine points to the need of strengthening an educational component, a clear strategy for the development of the educational component has not yet been developed and approved, and there is no understanding of resources allocated to achieve this task. The Ministry of Education and Science of Ukraine, together with the main cybersecurity entities, the private sector and other interested parties, should develop the National Strategy for development of Cybersecurity Human Resources (level 3). The strategy should provide for its constant updating and adjustment of implementation areas, a specific action plan for implementation;

✓ The State Employment Service should consider a possibility of introducing cybersecurity specialties (based on new educational standards of cybersecurity), as one of the for retraining for further confirmation of qualifications in the relevant Qualification Centers (level 3);

✓ The Ministry of Digital Transformation of Ukraine should develop cybersecurity courses focused on small and mid-sized businesses (level 4);

✓ For the Innovation Development Fund (Ukrainian Startup Fund) to provide as a condition for grant assistance for small and mid-sized businesses a mandatory requirement for grantees to have confirmed completion of relevant educational activities of the Ministry of Digital Transformation of Ukraine (level 4);

✓ The Ministry of Education and Science of Ukraine to recommend to higher education institutions of all forms of ownership to include in educational programs of training specialists in all areas at least short thematic (related to a specific specialty) cybersecurity courses (where appropriate: information protection, work with personal data, etc.) (level 4);

✓ To the Ministry of Education and Science of Ukraine to launch an all-Ukrainian expert assessment (in the form of an annual report with recommendations) to assess the shortcomings of professional training in the field of cybersecurity. The assessment should include specific offers to improve educational/training programs based on current cybersecurity challenges in Ukraine, as well as forecasts of such challenges (level 4 and 5).

Goal 8 – to facilitate research and development work

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Have studies or analyses been conducted to determine cybersecurity prioroties of Research & Development Works (R&D)?	1	Is there a process for setting cybersecurity priorities of R&D (e.g., new capabilities to deter, protect, detect, and adapt to new types of cyberattacks)?	1	Is there an understanding at the state level of how to link R&D projects to the real economy?	1	Are R&D projects related to cybersecurity aligned with relevant strategic goals, such as the Cybersecurity Strategy of Ukraine?	1	Does Ukraine cooperate at the national level with any international R&D projects related to cybersecurity?	1
2			Is the private sector involved in the formation of R&D priorities?	1	Are there any national projects related to cybersecurity?	1	Is there an evaluation framework for R&D projects?	1	Are R&D priorities coordinated with current or future regulations (at the national level)?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
3			Is the scientific community involved in a formation of R&D priorities?	1	Does Ukraine have local/regional startup ecosystems and other channels of interaction (e.g., technology parks, innovation clusters, networking events/ platforms) to promote innovation, including for cybersecurity startups?	1	Are there any cooperation agreements among state agencies and universities as well as other research institutions?	1	Is Ukraine involved in leading discussions on one or more of the leading R&D topics at the international level?	0
4			Are there any national R&D projects related to cybersecurity?	0	Are funds invested in cybersecurity R&D programs in the scientific community and the private sector?	1	Is there a recognized institutional agency that monitors cybersecurity research and development activities?	0		
5					Are there centers for scientific and industrial research at universities to combine research topics and market needs?	1				
6					Are there any special programs for financing R&D in the field of cybersecurity?	0				

Recommendations

✓ When approving R&D works related to various aspects of cybersecurity, the National Academy of Sciences of Ukraine should require the authors to indicate the impact of this R&D works on the real economy. The NCCC should establish a separate working group for periodic consultations with representatives of the scientific community engaged in relevant cybersecurity R&D works in order to improve the quality of coordination of research processes and better understand an expected impact of R&D results on the economy and the cybersecurity sector (level 3);

✓ The National Academy of Sciences of Ukraine should develop and approve a methodology for evaluating R&D projects that are directly related to cybersecurity. The assessment should include a ranking of projects in terms of their importance, type (fundamental/applied), an area of focus, etc. In future, the results of this assessment can be used by state agencies to determine expenditures for cybersecurity research and to seek additional international assistance for their implementation (level 4);

✓ The NCCC, together with the National Academy of Sciences of Ukraine, should determine (and, if necessary, create) an agency (possibly in a form of a permanent multidisciplinary group) that will monitor research activities in the field of cybersecurity.

Goal 9 – to encourage private sector to invest in security measures

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan regarding the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaption of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the excepted results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Is there an existing industrial policy or political will to encourage development of the cybersecurity industry?	1	Is the private sector involved in development of cyber security incentives?	1	Are economic, regulatory, or other types of incentives implemented to promote investment in cybersecurity?	1	Are there private enteties who respond to incentives by investing in security measures? For example, investors specializing in cybersecurity and non-specialized investors.	1	Does the government focus on cybersecurity initiatives in accordance with the latest threat developments?	1
2			Are there specific cybersecurity components/fields to be developed? For example, cryptography,	0	Is there support (e.g., tax incentives) for cybersecurity startups and small and mid-sized enterprises?	1	Does the government encourage the private sector to focus on the security of advanced technologies? For	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2			privacy, a new form of authentication, AI for cybersecurity, etc.	0			example, 5G, artificial intelligence, internet products, quantum computing, etc.	1		
3					Are tax benefits or other financial incentives provided to private sector investors in cybersecurity startups?	1				
4					Does the government facilitate access to government procurement for cybersecurity startups and small and mim-sized enterprises?	0				
5					Does the government have the budget to stimulate the private sector?	0				

Recommendations

✓ at the regulatory level, in particular through the law defining basic principles of information society development, the Budget Code of Ukraine, etc., to define the following: key types of economic, regulatory or other types of incentives to promote investment in cybersecurity; support measures (e.g., tax benefits) for startups and small and mid-sized businesses (SMBs) engaged in cybersecurity; tax benefits or other financial incentives for private sector investors supporting cybersecurity startups; possible government support measures for better access of startups and SMBs engaged in cybersecurity to the government procurement process; budgetary incentives for the private sector to develop cybersecurity. Incentive measures should also include a separate focus on the cybersecurity of advanced technologies, such as 5G, artificial intelligence, Internet products, quantum computing, etc. (level 4);

✓ annually review the status of implementation and effectiveness of these incentives with offers for their revision/modernization. This review should be prepared with a direct involvement of private sector representatives who either work in the field of cybersecurity or invest in such activities (level 5).

Goal 10 – to enhance supply chain cybersecurity

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan regarding the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaption of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the excepted results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Has research been conducted on security best practices in supply chain management used for procurement in various industry segments and/or the state sector?	1	Are cybersecurity assessments conducted along the entire supply chain of ICT (Informational Communication Technology) services and products in critical	1	Is a security certification scheme used for ICT-based products and services? For example, such as the European Common Criteria Recognition Agreement (CCRA), national projects, industry projects, etc.	1	Is there an implemented process for updating cybersecurity assessments in the supply chain of ICT services and products in critical sectors (as defined in Appendix II of the NIS Directive (2016/1148))?	1	Are there so called detection probes in key elements of the supply chain to detect early signs of disruption? For example, security control at an Internet service provider level, security probes in key infrastructure components, etc.	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
1			sectors (as defined in Appendix II to the NIS Directive (2016/1148))?	1						
2			Are standards used in the procurement policies of state administrative agencies to ensure that suppliers of ICT products or services meet basic information security requirements? For example, ISO/IEC 27001 and 27002, ISO/IEC 27036, etc.	1	Does the government actively promote data security and privacy by creating best practices for the development of ICT products and services? For example, a secure software development life cycle, a life cycle of Internet products.	1	Is there an implemented process for identifying cybersecurity weaknesses in the supply chain of critical sectors (as defined in Appendix II of the NIS Directive (2016/1148))?	1		
3					Are centralized catalogs with extensive information on available information security and privacy standards that are scalable for SMEs and used by them developed and made available?	1	Are mechanisms implemented to ensure that ICT products and services critical to basic service operators are cyber resilient (i.e., able to maintain availability and security against cyber incidents)? For example, through testing, regular assessments, detection of damaged elements, etc.	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
4					Is the government involved in development of the EU Guidelines for the Certification of Digital ICT Products, Services and Processes?	0	Does the government facilitate development of certification schemes aimed at small and mid-sized businesses to improve information security and adopt privacy standards?	0		
5					Are small and mid-sized businesses provided with any encouragement to adopt security and privacy standards?	0	Are there any developed regulations that encourage large companies to increase the cybersecurity of small businesses in their supply chains? For example, an online cybersecurity hotspot, training and awareness campaigns, etc.	0		
6					Are software providers encouraged to support small and mid-sized businesses through more secure configurations by customization in products targeted at small organizations?	0				

Recommendations

✓ to provide for a separate section on supply chain cybersecurity in the updated Cybersecurity Strategy of Ukraine with relevant tasks in the Action Plan for the Strategy implementation;

✓ The NCCC should initiate an expert study on the best security practices in a field of supply chain management used in procurement in various industry segments and/or in the state sector of leading countries;

✓ The NCCC should initiate an expert research on supply chain cybersecurity assessment in accordance with a list of critical infrastructure sectors defined by the Law of Ukraine «On Critical Infrastructure» and the Resolution of the Cabinet of Ministers of Ukraine No. 1109 of October 9, 2020. Based on the results of the research, together with cybersecurity entities, assess cybersecurity in the supply chain of ICT services and products in critical sectors;

✓ it is advisable to consider the need to introduce a system of reporting by critical infrastructure facilities (at least 1-2 categories) to a designated state agency on key elements of the supply chain regarding which the critical infrastructure facilities monitor possible violations and what measures are taken to prevent attacks through such elements. For example, make it as a part of the Critical Infrastructure Facilities passport;

✓ The State Service of Special Communications and Information Protection of Ukraine, together with other authorized agencies, to develop and publish guidelines for documenting supply chains of organizations, main methods of their protection (security) andtesting. These guidelines should be segmented by targetaudiences: small and mid-sized businesses, CI operators, and state agencies;

✓ to establish mandatory requirements for assessing a state of cybersecurity for organizations that provide services to Critical Infrastructure Facilities of categories 1-2;

✓ The NCCC, together with the State Special Communications Service and Information Protection of Ukraine, should initiate a research on a possibility of Ukraine's accession to the European Framework for Certification of Digital Products, services and processes of Information and Communications Technology, and, if possible, start a dialogue with the EU authorized agencies on jengaging in this process;

✓ together with representatives of large business companies, work on the issue of establishing additional incentives (or restrictive measures) for small suppliers («SMBs») to ensure their compliance with cybersecurity requirements. Evaluate the possibility of providing additional incentives for large business organizations to introduce increased cybersecurity requirements for their suppliers;

✓ together with software providers that are actively used by small and mid-sized businesses, consider a possibility of creating additional special support programs for such entities to strengthen their cybersecurity.

Goal 11 – protection of critical informational infrastructure (CII), basic service operators and digital service providers

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Is there a general understanding that CII operators contribute to national security?	1	Do you have a methodology for determining core services?	1	Has the NIS Directive (2016/1148) been implemented?	1	Is there a procedure for updating a risk register?	1	Are threat environment reports created and updated?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2			Is there a methodology for identifying CII?	1	Has the EU Directive (2008/114) on the identification and designation of European critical infrastructures and an assessment of the need to improve their protection been implemented?	1	Are there other implemented mechanisms to measure whether technical and organizational measures implemented by basic service operators are adequate to manage a risk facing network and information system security? For example, regular cybersecurity audits, national guidelines for implementing standardized measures, technical tools provided by the government, such as detection probes or system-specific configuration analysis, etc..	1	Depending on the latest developments in the threat environment, is there a possibility to include a new sector in the national CII protection action plan?	1
3			Is there a methodology for determining basic service operators?	1	Is there a national register of basic service operators in each of the critical sectors?	1	Is a list of designated basic service operators analyzed and updated at least once every two years?	1	Depending on the latest events in the threat environment, is there a possibility to add new requirements to the CII protection action plan?	1
4			Is there a methodology for identifying digital service providers?	1	Is there a national register of designated digital service providers?	1	Are there implemented mechanisms to measure whether technical and organizational measures implemented by digital service providers are	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
4							adequate to manage a risk facing network and information system security? For example, regular cybersecurity audits, national guidelines for implementing standardized measures, technical tools provided by the government, such as detection probes or system-specific configuration analysis, etc.	1		
5			Are there one or more national agencies responsible for monitoring protection of critical information infrastructure and security of networks and information systems? For example, as required by the NIS Directive (2016/1148).	1	Is there a national risk register for identified or recognized risks?	1	Is a list of designated digital service providers analyzed and updated at least once in every two years?	1		
6			Are sectoral protection plans being developed? For example, basic cybersecurity measures (mandatory or advisory).	0	Is there a methodology for mapping CII interdependencies?	1	Is the security certification scheme (national or international) used to assist basic service operators and digital service providers to identify secure Infornational Communications Technology products?	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
7					Are risk management practices implemented to identify, quantify, and manage CII-related risks at the national level?	1	Is the security certification scheme or qualification procedure used to evaluate service providers that work with basic service operators? For example, service providers in the fields of incident detection, incident response, cybersecurity auditing, cloud services, computerized maps, etc..	1		
8					Does Ukraine participate in a consultation process to identify cross-border interdependencies?	1	Are mechanisms implemented to measure a level of compliance of basic service operators and digital service providers with respect to basic cybersecurity measures?	0		
9					Is there a single coordinator responsible for coordinating issues related to the security of network and information systems at the national level and within the framework of cross-border cooperation?	1	Are there implemented regulations to ensure continuity of services provided by critical information infrastructures? For example, crisis anticipation, procedures for restoring critical information systems, business continuity	0		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
9							without IT, procedures for backing up and moving data offline, etc.	0		
10					Are basic cybersecurity measures (mandatory or advisory) defined for digital service providers and all sectors defined in Appendix II of the NIS Directive (2016/1148)?	1				
11					Are tools or methodologies provided to detect cyber incidents?	0				

Recommendations

✓ to create the National Risk Register and approve the procedure for its constant updating;

✓ The State Service of Special Communications and Information Protection of Ukraine should develop a methodology and, on its basis, conduct a periodic study to map CII interdependencies. On the basis of this research to start a dialogue with the European partners to study similar cross-border interdependencies;

✓ to organize an annual consolidated public report on the threat environment (preferably based on the ENISA methodology);

✓ The NCCC and The State Service of Special Communications and Information Protection of Ukraine to start a dialogue with ENISA (as the developer of the methodology for assessing the level of national capabilities) on modernizing the methodology in terms of implementing provisions of the NIS Directive and replacing these tasks with implementation of Directives 2555/2557;

✓ to consider feasibility of introduction of a certification procedure for those service providers who work directly with Critical Infrastructure Facilities (in particular, cybersecurity service providers);

✓ to introduce mandatory requirements for all Critical Infrastructure Facilities to have Business Contingency Plans. The State Service of Special Communications and Information Protection of Ukraine, together with other key entities, should develop standard plans and a methodology for their application.

Goal 12 – to counteract cybercrime

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Has research been conducted to determine a state of law enforcement agencies' capabilities (legal framework, resources, skills, etc.) to effectively combat cybercrime?	1	Is the national legislative framework fully compliant with the relevant EU legislative framework, including Directive 2013/40/EU on attacks on information systems? For example, illegal access to information systems, illegal interference	1	Are there any units responsible for countering cybercrime in the prosecutor's office?	1	Are statistics collected in accordance with provisions of the Article 14(1) of the Directive 2013/40/EU (Directive on attacks on information systems)?	1	Is there inter-agency training or exercises for law enforcement agencies, judges, prosecutors and the national/state CSIRT teams at the national level and/or multilateral level?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
1			with the system, illegal interference with data, illegal interception, tools used to commit offenses, etc.	1						
2	Has research been conducted to identify requirements for prosecutors and judges (legal framework, resources, skills, etc.) to effectively counter cybercrime?	1	Is there any legislative regulation regarding online identity theft and personal data theft?	1	Is there a special budget allocated to cybercrime units?	1	Are specific statistics collected on cybercrime? For example, operational statistics, statistics on cybercrime trends, statistics on cybercrime income and losses, etc.	1	Does Ukraine participate in coordinated actions at an international level to disrupt criminal activities? For example, infiltration of criminal hacker forums, organized groups of cybercriminals, dark websites and elimination of botnets, etc.	1
3	Has Ukraine signed the Budapest Convention on Cybercrime of the Council of Europe?	1	Are there any legislative regulations regarding intellectual property and copyright infringement on the Internet?	1	Has a central agency/ organization been established to coordinate cybercrime activities?	1	Is an appropriateness of training for law enforcement agencies, justice, and the national CSIRT team personnel on cybercrime issues assessed?	1	Is there a clear assignment of responsibilities among the CSIRT team, law enforcement agencies and justice (prosecutors and judges) when they work together to counteract cybercrime?	1
4			Are there any legislative regulations regarding online harassment or cyberbullying?	1	Are cooperation mechanisms established among relevant national institutions involved in a counteraction against cybercrime, including law enforcement agencies, national CSIRT teams?	1	Are regular assessments conducted to ensure that the country has sufficient resources (human, budgetary and instrumental) allocated to cybercrime units within the law enforcement system?	1	Is the regulatory framework conducive to cooperation among CSIRT teams/law enforcement agencies and judiciary (prosecutors and judges)?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
5			Is there any legislative regulation to counteract computer fraud? For example, compliance with the Council of Europe's Budapest Convention on Cybercrime.	1	Is there any cooperation and exchange of information with the EU member countries in the field of countering cybercrime?	1	Are regular assessments carried out to ensure that the country has sufficient resources (human, budgetary and instrumental) allocated to cybercrime units within the prosecutor's office?	1	Does Ukraine participate in a creation and maintenance of standardized tools and methodologies, forms and procedures that can be shared with international partners (law enforcement agencies, CSIRT, ENISA, Europol EC3 teams, etc.)?	1
6			Are there any legislative regulations to protect children online? For example, compliance with the Directive 2011/93/EU and the Council of Europe's Budapest Convention on Cybercrime.	1	Does Ukraine cooperate and exchange information with the EU agencies (e.g. Europol EC3, Eurojust, ENISA) in the field of countering cybercrime?	1	Are there any units, specialized courts or judges that deal with cybercrime cases?	1	Are there any progressive mechanisms to deter people from engaging in or participating in cybercrime?	0
7			Has an operational national coordinator been identified to exchange information and respond to urgent information requests from the EU Member Countries regarding offenses under the Directive 2013/40/EU (Directive on attacks on information systems)?	1	Are there appropriate tools to counteract cybercrime? For example, taxonomy and classification of cybercrime, tools for collecting electronic evidence, computer forensics tools, reliable exchange platforms, etc.	1	Are there any regulations on providing support and assistance to victims of cybercrime (general users, small and mid-sized businesses, large companies)?	1	Does Ukraine use the EU Law Enforcement Emergency Response Concept and/or Protocol (EU LE ERP) to effectively respond to large-scale cyber incidents?	0

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
8			Is there a special cybercrime unit within the national law enforcement agency?	1	Are there standard operating procedures for processing electronic evidence?	1	Are interagency frameworks and cooperation mechanisms established among all relevant parties (e.g., law enforcement agencies, the national CSIRT team, justice, community), including the private sector (e.g., basic service operators, service providers), where appropriate, to respond to cyber attacks?	1		
9			Has a 24-hour coordinator been appointed in accordance with the Article 35 of the Budapest Convention?	1	Does Ukraine participate in professional development opportunities offered and/or supported by the EU agencies (e.g. Europol, Eurojust, European Anti-Fraud Office, Cepol European Police College, ENISA)?	0	Does the Ukrainian regulatory framework facilitate cooperation between the CSIRT teams and law enforcement agencies?	1		
10			Has an operational, 24-hour national coordinator been appointed for the EU Law Enforcement Emergency Response Protocol (EU LE ERP) to respond to large-scale cyber-attacks?	1	Does Ukraine plan to adopt the 2nd Additional Protocol to the Budapest Convention on Cybercrime of the Council of Europe?	0	Are there mechanisms (e.g., tools, procedures) implemented to facilitate information sharing and cooperation among the CSIRT teams/law enforcement agencies and possibly the justice	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
10							(prosecutors and judges) in the counteraction against cybercrime?	1		
11			Is there regular specialized training for interested parties involved in countering cybercrime (law enforcement agencies, justice, and the CSIRT team)? For example, but not limited to, training on registering/prosecuting cybercrime, training on collecting electronic evidence and ensuring integrity throughout the digital chain of custody and computer forensics.	1						
12			Has Ukraine ratified/ joined the Budapest Convention on Cybercrime of the Council of Europe?	1						
13			Has Ukraine signed and ratified the Additional Protocol (criminalization of acts of a racist and xenophobic nature committed through computer systems) to the Budapest Convention on Cybercrime of the Council of Europe?	0						

Recommendations

✓ to consider establishing specialized courts (or additionally trained judges) to deal with cybercrime cases (level 4);

✓ to conduct regular information campaigns to prevent involvement of citizens in cybercrime activities.

Goal 13 – to establish incident report mechanisms

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
1	Are there any informal mechanisms for exchanging information on cybersecurity incidents between private organizations and state agencies?	1	Is there an incident reporting scheme for all sectors in accordance with Appendix II of the NIS Directive?	1	Is there a mandatory incident reporting scheme that functions in actual practice?	1	Is there a harmonized procedure for industry-specific incident reporting schemes?	1	Is an annual incident report issued?	1
2			Have notification requirements for telecommunication service providers been implemented in accordance with the Article 40 of the Directive (EU 2018/1972)? The Directive requires countries to ensure that providers of public electronic data networks or public electronic communications services notify the competent authority without undue delay of a security incident that has a significant impact on the operation of the networks or services.	1	Is there a coordination/ cooperation mechanism for incident reporting obligations in terms of the GDPR, NIS Directive, Article 40 (former Article 13a) and eIDAS?	1	Is there an incident reporting scheme for sectors other than those covered by the NIS Directive?	1	Are there any cybersecurity environment reports or other types of analysis prepared by an organization that receives incident reports?	1
3			Are there notification requirements for trust service providers under the Article (19) of the eIDAS Regulation	1	Are there any tools to ensure confidentiality and integrity of information transmitted through various reporting	1	Is the effectiveness of incident reporting procedures measured? For example, the percentage of incidents	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
3			(Regulation (EU) No 910/2014)? The Article (19), among other requirements, requires trust service providers to report significant incidents/breaches to the supervisory authority.	1	channels at the national level?	1	reported through the appropriate channels, time of reporting an incedent report, etc.	1		
4			Have notification requirements for digital service providers been implemented in accordance with the Article (16) of the NIS Directive? The Article (16) requires digital service providers to notify a competent authority or the national CSIRT team without undue delay of any incident that significantly affects provision of the service as defined by Appendix III.	1	Is there a platform/tool to simplify the reporting process?	0	Is there a general systematization at the national level for classifying and categorizing incidents?	0		

Recommendations

✓ to introduce an obligation for telecommunication service providers to notify a competent agency of a cybersecurity incident that had a significant impact on the functioning of their (the provider's) networks or services (level 2);

✓ to establish an interagency coordination mechanism for mandatory incident reports (including incidents related to personal data security, electronic identification problems, etc.) to be submitted to the authorized agencies (level 3);

✓ to develop a methodology for assessing effectiveness of cyber incident reporting, including measuring formal indicators: reporting time, use of reporting channels, etc.

Goal 14 – to strengthen data privacy protection

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan regarding the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaption of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the excepted results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Has research or analysis been conducted to identify fields of improvement to better protect citizens' privacy rights?	1	Is the national data protection agency involved in cybersecurity-related issues (e.g., drafting new laws and regulations on cybersecurity, defining minimum security measures)?	1	Are best practices for data security and protection measures promoted specifically for the state and/or private sector?	1	Are regular assessments carried out to ensure that the country has sufficient resources (human, budgetary and instrumental) dedicated to the data protection agency?	1	Are there any implemented mechanisms to monitor the latest technological developments in order to adapt relevant guidelines and legislative provisions/obligations?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2	Has the national legal framework been developed to ensure the implementation of the General Data Protection Regulation (EU Regulation 2016/679)? For example, supporting or introducing more specific provisions or limitations to the Regulation.	0			Are there any awareness-raising and training programs on this topic?	1	Are organizations and businesses encouraged to get certified for compliance with ISO/IEC 27701:2019 on the Information Security Management System for Sensitive Data (ISMS)?	1	Does Ukraine actively participate in (or contribute to) R&D projects on privacy enhancing technologies (PETs)?	0
3					Are incident reporting procedures coordinated with provisions of personal data protection legislation?	1				
4					Is development of technical standards for information security and privacy facilitated/ supported? Are they specifically designed for SMEs?	0				
5					Is practical guidance provided to support different types of data controllers in meeting their legal requirements and obligations regarding privacy and data protection?	0				

Recommendations

✓ to provide for a separate section on personal data security in the updated Cybersecurity Strategy of Ukraine with relevant tasks in the Action Plan for the implementation of the Strategy;

✓ to assess the existing legislative framework and prepare appropriate amendments to it to ensure implementation of the General Data Protection Regulation (EU Regulation No. 2016/679) (level 1);

✓ to take necessary steps to ensure that cyber incident reporting procedures take into account the need to report incidents involving loss of personal data in case of such incidents;

✓ To the Authorized Representative of Verkhovna Rada of Ukraine for Human Rights to conduct an annual assessment of a situation with personal data protection (in particular, regarding adequacy of resources of state agencies for such activities) in the state sector;

✓ when updating legislation on development of data protection systems (including information security management systems), provide for mandatory consideration of the main provisions and requirements of ISO/IEC 27701:2019;

✓ The National Academy of Sciences of Ukraine, together with other interested parties, should implement research programs aimed at developing PETs (privacy enhancing technologies), including but not limited to end-to-end encryption, VPNs, etc..

Goal 15 – to establish public-private partnership (PPP)

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Is it generally accepted at the country level that PPP contribute to improving cybersecurity in the country through various means? For example, joint actions based on common interests to grow the cybersecurity industry, cooperation in creating an appropriate regulatory framework for cybersecurity, promoting R&D, etc.	1	Is there a national action plan for establishing the PPP?	1	Are there any specific examples of public-private partnership at the national level?	1	Are there any specific examples of the cross-sector PPP?	1	Depending on the latest technological and regulatory developments, can you adapt or create the PPP?	1
2			Is legal or contractual basis defined (specific laws, non-disclosure agreements, intellectual property) for covering the PPP?	1	Are there any specific examples of the PPP that are specific to a particular industry?	1	Are there any examples of focusing on interagency (G2G) and business-to-business (B2B) cooperation mechanisms within the existing PPP mechanisms?	1		

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
3					Does the state fund specific elements of the PPP?	1	Is there any assistance for the creation of the PPP among small and mid-sized enterprises?	1		
4					Do state agencies generally lead the PPP process, i.e., is there a single state sector coordinator who manages and coordinates the PPP, do state agencies agree in advance on what they want to achieve, are there clear guidelines from state administrative agencies on their needs and limitations for the private sector, etc.	1	Are the results of the PPP measured?	1		
5					Is Ukraine (state agencies) a member of international organizations that aim to promote the PPP? For example, the European Cyber Security Organization (ECSO) or other similar organizations.	0				
6					Is there one or more PPPs in Ukraine that work within the framework of the CSIRT team?	0				

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
7					Is there one or more PPPs in Ukraine working on the protection of critical information infrastructure?	0				
8					Is there one or more PPPs in Ukraine working to raise awareness and develop skills in cybersecurity?	0				

Recommendations

✓ to develop and adopt the Law on public-private partnership in the field of cybersecurity, as well as the National PPP Strategy for the practical implementation of the law's provisions. The law should also define specific legal forms of the PPP in the field of cybersecurity and logic of implementing such projects. (Level 2). The National Strategy should separately provide for a clear and understandable process for engaging SMBs in the PPP activities;

✓ to create (on the basis of the NCCC, the State Service of Special Communications and Information Protection of Ukraine or another key entity of the national cybersecurity system) common database of needs of state institutions for projects that can be implemented in the PPP format. State agencies planning the PPP activities should include funds for such projects in their budgets or receive confirmation of a possibility to attract such funds from international technical assistance projects (level 3);

✓ The national strategy should be reviewed periodically. This review should involve representatives of both the state and the private sector.

Goal 16 – to institutionalize cooperation among state agencies

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaptation of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goa been implemented to at least a limited scope?	0						
1	Are there informal channels of cooperation among state agencies?	1	Is there a national cooperation scheme focused on cybersecurity? For example, advisory councils, coordination groups, forums,councils, cyber centers, or expert groups.	1	Are state agencies involved in such cooperation schemes?	1	Are there channels of cooperation in a field of cybersecurity provided/ created among at least the following state agencies: intelligence agencies, domestic law enforcement agencies, prosecutors, government entities, the national CSIRT team, and the military?	1	Are state agencies provided with summarized minimum information on the latest developments in the threat environment and situational awareness of cybersecurity?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2					Have cooperation platforms been created to share information?	1	Are the progress and limitations of different cooperation schemes measured?	1		
3					Is a scope of the cooperation platform defined (e.g., tasks and responsibilities, number of problematic fields)?	1				
4					Are annual meetings organized to establish cooperation?	1				
5					Are there mechanisms for cooperation among relevant agencies at the regional level? For example, a network of security experts by region, cybersecurity officers in regional Chambers of Commerce, etc.	1				

Recommendations

✓ while cooperation among cybersecurity experts at the national and capital levels is mostly established, at the regional level, vertical and horizontal connections are still insufficient. It is important to create a format of permanent regional platforms for cybersecurity experts, where they could discuss specific regional cybersecurity issues and communicate with central government officials in a consolidated manner.

Goal 17 – to engage in international cooperation (not only with the EU member countries)

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
a	Does the current National Cybersecurity Strategy include a task of developing National Cybersecurity Incident Response Plans or are there plans to include them in a future version of the strategy?	1	Are there informal practices or measures that are used to achieve the Goal in an uncoordinated way?	1	Does Ukraine have an officially defined and documented action plan (regarding the Goal)?	1	Is the action plan in regard the Goal tested to see if it is effective?	1	Does Ukraine have implemented mechanisms to ensure dynamic adaption of the action plan regarding the Goal in accordance with changes in the environment?	1
b			Are the expected results, guiding principles or key activities identified in the action plan regarding the Goal?	1	Does Ukraine have the action plan regarding the Goal (or the National Plan itself) that clearly allocates and manages resources?	1	Is the action plan regarding the Goal reviewed to ensure that it is properly optimized and prioritized?	1		
c			Has the action plan regarding the Goal been implemented to at least a limited scope?	0						
1	Is there a strategy for international cooperation?	1	Does Ukraine have cooperation agreements with other countries (bilateral, multilateral) or partners in other countries? For example, on information exchange, capacity building, assistance, etc.	1	Is information shared at a strategic level? For example, regarding a high-level of cybersecurity policies, risk perception, etc.	1	Are state cybersecurity agencies involved in international cooperation programs?	1	Are at least one or more topics being discussed under multilateral agreements?	1

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2	Are there any informal channels of cooperation with other countries?	1	Is there a single coordinator who can act as a liaison to ensure cross-border cooperation with member state agencies (cooperation group, CSIRT team network, etc.)?	1	Does Ukraine share information at the tactical level? For example, information about attackers, Information Sharing and Analysis Centers (ISACs), tactics, methods and procedures, etc.	1	Is there a regular assessment of the results of international cooperation projects?	1	Is one or more topics discussed under international treaties or conventions?	1
3	Has the government expressed its intention to participate in international cooperation in cybersecurity?	1	Are there any designated specialists involved in international cooperation?	1	Does Ukraine exchange information at the operational level? For example, information on operational coordination, current incidents, IOC controllers, etc.	1			Are there discussions or negotiations on one or more topics within international expert groups? For example, the Global Commission on Cyberspace Stability (GCSC), the ENISA NIS Collaboration Group, the UN Group of Governmental Experts (GGE)).	1
4					Does Ukraine participate in international cybersecurity trainings?	1				
5					Does Ukraine participate in international capacity-building projects? For example, trainings, skills development programs, drafting standard procedures, etc.	0				

	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
6					Have mutual assistance agreements been signed with other countries? For example, law enforcement agencies, judicial proceedings, combining incident response capabilities, sharing cybersecurity assets, etc.	0				
7					Are international treaties or conventions in the field of cybersecurity signed or ratified? For example, the International Code of Conduct regarding Information Security, the Convention on Cybercrime.	0				

According to a high level of indicators, there are no recommendations regarding the Goal 17 "engage in international cooperation (not only with EU member states)".