Ukrainian Cybersecurity
Legal Framework:
Overview and Analysis

The report provides a comprehensive overview and analysis of the existent Cybersecurity Legal Framework in Ukraine, its compliance with the international obligations and best practices, and recommendations on initial steps for improvement and potential international assistance needed.

Yuliya Shypilova*
International Foundation for Electoral Systems

*The author wishes to thank Thomas Chanussot and Juliette Schmidt for their valuable review and input to this report.
# Table of Contents

Executive Summary ........................................................................................................ 3

Introduction and Methodology .................................................................................... 5

International Obligations on Cybersecurity ................................................................. 6
  Budapest Convention .................................................................................................. 7
  NIS Directive ........................................................................................................... 10

National Legislation ...................................................................................................... 12
  Cybersecurity Strategy .............................................................................................. 13
    Cybersecurity strategy goals .................................................................................. 13
    Cyberthreats ........................................................................................................... 13
    Cybersecurity priorities ....................................................................................... 14
    Delineation of powers between cybersecurity agencies ......................................... 14
  Primary Legislation Level. Law on Cybersecurity ..................................................... 15
  Secondary Legislation Level .................................................................................... 18

Regulation on Critical Infrastructure Protection ......................................................... 20
  Concept of Critical Infrastructure Protection ......................................................... 20
  Draft Law on Critical Infrastructure Protection ...................................................... 21
  Drafts of Secondary Legislation ............................................................................. 23

Gaps and Ambiguities of the Current Legislation ....................................................... 25

Roadmap for Reforming Cybersecurity Legal Framework .......................................... 27

Legislative Framework on Cybersecurity in Ukraine ................................................. 29

Secondary Legislation on Cybersecurity in Ukraine .................................................. 29

List of Drafts Laws and Secondary Legislation .......................................................... 30
  Daft Laws Registered in the Verkhovna Rada of Ukraine of 8th Convocation ........... 30
  Daft Laws Registered in the Verkhovna Rada of Ukraine of 9th Convocation .......... 31
  Secondary Legislation Drafts .................................................................................. 31

Delineation of Powers between Ukrainian Authorities Responsible for Cybersecurity 32

Roles of Cybersecurity Agencies ............................................................................... 33
Executive Summary

The cybersecurity legal framework of Ukraine consists of international obligations and domestic legislation. Of particular note internationally are the Budapest Convention and the Network and Information Security (NIS) Directive. The commitments Ukraine has made, as a signatory of international treaties and conventions, or those it would need to make should it pursue aspirations to join the European Union, should be reflected in national legislation. Nationally, Law No 2163-VIII adopted of 5 October 2017 on the Main Principles of Maintaining Cybersecurity of Ukraine (hereinafter, the Law on Cybersecurity) and the Ukrainian National Cybersecurity Strategy are the predominant texts governing this space.

This assessment provides an analysis and comparison of these documents, identifying gaps and areas for improvement rooted in good practice, in order to improve and protect critical Ukrainian IT infrastructure.

In 2005 Ukraine ratified the Budapest Convention, the only binding international instrument on cybersecurity, which establishes a common criminal policy on cybercrime protection by adopting relevant domestic legislation and fostering international collaboration. However, not all its provisions have been integrated into national legislation and full implementation will require significant amendments to the Code of Criminal Procedure.

In 2016 the European Parliament adopted the first piece of EU-wide legislation on cybersecurity – the NIS Directive. As Ukraine is not part of the EU, the NIS Directive is not binding; however, it serves as a good practice guide. While some of the provisions have been voluntarily implemented in Ukrainian legislation, others remain unaddressed.

In recent years, Ukraine has adopted a number of acts governing cybersecurity issues which constitute its national cybersecurity legal framework. In 2016 Ukraine’s National Cybersecurity Strategy identified goals and priorities for cybersecurity through 2020. Its provisions were reinforced in the Law on Cybersecurity adopted in 2017. The latter identifies important terms, delineates powers between cybersecurity agencies and defines principles for the full regulation of Critical Infrastructure (CI) protection and public-private partnership.

The adoption of the Law on Cybersecurity was a welcome step; however, much effort is still needed to fully implement all its aspects. Most importantly, the government has not yet adopted the by-laws (or secondary legislation) identified by the Law on Cybersecurity within the legal deadlines, most notably those regulating the protection and audit of CI objects (the specific pieces of hardware and software that comprise and support CI). As a consequence, many legal provisions remain vague, not defining the necessary procedures.

Ukrainian authorities have not yet decided how they intend to regulate CI protection issues and are currently considering whether to do so at the primary or secondary legislation level. The Ministry of Economic Development and Trade developed a Draft Law on CI and its Protection, which was registered at the Verkhovna Rada’s 8th convocation, but not considered; hence it is deemed to have been withdrawn. Given the change of government in Ukraine, the chances for adoption of the draft in the near future are quite low. The State Service of Special Communications and Information Protection (SSSCIP) developed drafts for secondary legislation regulating CI protection issues, but it is also unlikely that they will be approved in the next few months.

As different laws governing cybersecurity were adopted at different times, terminology is used
inconsistently and there is no clarity in the delineation of powers between cybersecurity agencies; thus the full Ukrainian cybersecurity legal framework requires careful review. In addition, there are a number of gaps and ambiguities in the legislation. Significant issues include:

- Lack of harmonization between domestic legislation and international commitments;
- Inconsistency in terminology and lack of CI regulations;
- Absence of regulations on CI information security audits;
- Jurisdictional overlap;
- Absence of clear requirements for CI administrators and digital service providers to report cyber incidents;
- Lack of a cybersecurity strategic plan; and
- Fiscal constraints that limit the government’s ability to pay competitive wages to attract and retain the cybersecurity workforce they need.

Over the past few years, Ukraine has taken a number of positive steps to implement its international commitments and improve cybersecurity legislation; however, much effort is still needed. Initial areas for improvement include:

- Further elaboration of existing legislation to address gaps and irregularities in line with international commitments, in particular, further compliance with the Budapest Convention and NIS Directive;
- Development and adoption of comprehensive legislation on cybersecurity, laying out consistent terminology, incident notification requirements, and legislation on public-private partnerships;
- New by-laws on establishing common criteria and methodology for the assignment of infrastructure as critical, and procedures for certification, categorization and audit. The adoption of the Law on CI and its protection should be a priority;
- Clarification on areas of jurisdictional overlap through changes to procedural and substantive law;
- Clarification of the features of cybercrimes qualifying them as crimes;
- Differentiation of jurisdiction and criminal responsibility for cybercrimes targeting state or information resources, critical infrastructure and other objects; and
- An updated Cybersecurity Strategy and Ukrainian cybersecurity strategic plan.
Introduction and Methodology

In recent years, Ukraine has encountered several waves of cyberattacks which have caused serious damage to its infrastructure and raised concerns over the preparedness of the country, particularly in the context of the hybrid war perpetrated by the Russian Federation. While the technical preparedness and capacity of the cybersecurity staff plays an important role, it needs to be complemented by an adapted legislation with regards to cyber protection.

Cybersecurity is a complex issue. Its regulation is a complicated task for any country, and Ukraine is no exception. This overview of cybersecurity legal framework in Ukraine aims to examine the existing international and national legal framework that governs cybersecurity, assess the national legislation on compliance with international obligations and best practices, and identify gaps and inconsistencies which would require developing new laws or amending the current legislation.

This report outlines the main legal acts to provide an overall picture of cybersecurity regulations, the current powers of cybersecurity agencies, and positions and interests of key cybersecurity stakeholders on amending existing legislation and changing the status quo. It also offers a short blueprint of activities to improve the legal framework and cybersecurity system in accordance with international standards and best practices.

Ukraine has signed a number of international treaties committing to ensure security in cyberspace. Such international obligations serve as a baseline for further legal regulation of cybersecurity issues. By signing these treaties, Ukraine has committed itself to certain standards and assumed the obligations to implement them as part of the national legislation. This overview assesses Ukraine's progress in fulfilling international cybersecurity commitments and identifies further steps in the implementation of international standards and best practices in the Ukrainian legislation.

While Ukraine is not a member of the EU and thus has not signed the NIS Directive, Ukrainian authorities are largely aware of its provisions and requirements, which have been reflected to some extent in the national legislation and cybersecurity systems. This overview pays attention to Ukraine's compliance with the NIS Directive and labels areas requiring international assistance on further implementation in the national legislation.

In recent years, Ukraine has made significant steps forward in establishing a cybersecurity legal framework. In 2016 Ukraine adopted the Cybersecurity Strategy of Ukraine which identifies the priorities and directions for cybersecurity and is an important pillar for building a world class cybersecurity policy. This overview pinpoints the shortcomings of the current strategy and highlights the necessary improvements.

To implement the Cybersecurity Strategy, the Parliament of Ukraine adopted the Law on Cybersecurity - a pivotal law which sets up a legal framework for the cybersecurity system. The Law on Cybersecurity establishes the backbone of the cybersecurity system - the key national cybersecurity stakeholders and their roles, as well as coordination of cybersecurity activities. It also describes the CI protection in general terms and serves as the starting point for further regulation of CI. This overview also considers the draft regulations that have been proposed to further regulate CI protection.

Finally, the report's overview summarizes the gaps and ambiguities of the current legislation and defines the starting points for improvement, including potential international assistance. Such points could serve as the foundation for designing program activities and establishing a partnership with the relevant stakeholders.
International Obligations on Cybersecurity

Although cybersecurity is a crucially important field, there is no comprehensive global international treaty which sets forth international standards. As cyberspace is a relatively new phenomenon, global intergovernmental institutions have not adopted any binding treaties or conventions. The negotiation process on this issue is ongoing, and since different countries use different approaches even on terminology, it is slow and complicated. In 2011 and again in 2015 Russia and China tried to submit to the UN General Assembly a “Code of Conduct for Information Security”; however, it was not accepted. There is strong disagreement between China, Russia, and the US, so-called “cyber superpowers”, in terms of how cybersecurity rules should be regulated. Thus, the chances for the adoption of omnibus treaties in the near future are quite low.

In 2015, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security presented a report to the UN General Assembly. The report provides an analysis on existing and emerging threats; how international law applies in the use of ICTs; norms, rules and principles of responsible behavior by UN-participating states; confidence-building measures; international cooperation and assistance in ICT security; and capacity building. The report contains recommendations which serve as guidelines for countries on how to improve security in cyberspace.

The United Nations Convention Against Transnational Organized Crime (2000) is a global international treaty which partly regulates cybersecurity issues. Although it does not explicitly address cybercrime, its provisions are highly relevant as it sets up frameworks for extradition, mutual legal assistance, and law enforcement cooperation. Ukraine signed it in 2000 and ratified the document in 2004 with reservations. These reservations are: 1) “the Convention shall be applied only subject to the observation of the constitutional principles and fundamental basis of the legal system of Ukraine”, and 2) “the term «serious crime» corresponds to the terms «grave crime» and «especially grave crime» in Ukrainian criminal law”.

Another international document partly governing cybersecurity issues is the 1992 Constitution of the International Telecommunication Union. The treaty is the founding document of the International Telecommunication Union (ITU), a specialized agency of the UN. The Constitution was signed by all UN member countries, including Ukraine. It regulates maintenance and extension of cooperation with regard to the use of telecommunications internationally; development of facilities and efficiency of services in this field; and operations interfering with existing telecommunications networks. Each year ITU produces the Global Cybersecurity Index – a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. The ITU tracks progress globally by assessing country cyber-preparedness along five pillars: 1) legal measures; 2) technical measures; 3) organizational measures; 4) capacity building; 5) cooperation.

---

4 https://www.itu.int/council/pd/constitution.html.
5 According to 2018 Global Cybersecurity Index, Ukraine has 32nd place at the regional level and 54th at global level. As Ukraine is assigned to Europe, its rank is not high at regional level due to the better development of other European countries. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EVS_print_2.pdf.
Budapest Convention

The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention, is the only binding international instrument on this issue, describing itself as “the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception”. The Budapest Convention serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between state parties to this treaty. The Budapest Convention is supplemented by a protocol concerning “acts of a xenophobic and racist nature committed through computer systems” and a Guidance Note.

The Budapest Convention was adopted in 2001 and came into force in 2004. Ukraine ratified the convention in 2005 and stipulated some important reservations to this treaty, including whether to criminalize the production or use of programs or devices for the purpose of illegal access or interception, as well as data or system interference, under domestic law. Ukraine reserved the right not to apply paragraph 1 of Article 6 of the Budapest Convention, which prescribes that “…each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally and without right, the production, sale, procurement for use, import, distribution or otherwise making available of: 1. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses […] or 2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used for the purpose of committing any of the offenses […]”. By “offenses”, the Budapest Convention refers to violations prescribed by Articles 2-5: namely, illegal access, illegal interception, data interference and system interference.

On October 15, 2015, Ukraine made a declaration that starting from February 20, 2014, and for the period of temporary occupation by the Russian Federation of part of the territory of Ukraine – the Autonomous Republic of Crimea and the city of Sevastopol as well as certain districts of the Donetsk and Luhansk oblasts of Ukraine, which are temporarily not under control of Ukraine – the application and implementation by Ukraine of obligations under the Budapest Convention is limited and not guaranteed. It is worth mentioning that Russia is the only European country that did not sign the Budapest convention, partly because it allowed foreign law enforcement officials to directly query Internet service providers. Russia officially argued that the ratification of the Budapest Convention may violate Russian sovereignty. Moreover, Russia plans to offer a new UN cyber-regulation pact intended to be a cyber “code of conduct” and a pathway to a new cybercrime convention. Russia is conducting a quiet lobbying campaign for its UN package by organizing and sponsoring events devoted to discussion of cybercrimes.

The Budapest Convention identifies the following offenses which were implemented in Ukrainian criminal legislation:

<table>
<thead>
<tr>
<th>Type of offense</th>
<th>Article of Budapest Convention</th>
<th>Article of the Criminal Code of Ukraine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegal access</td>
<td><strong>Article 2:</strong> The accessing of the whole or any part of a computer system without right.</td>
<td>359, 361</td>
</tr>
<tr>
<td>Illegal interception</td>
<td><strong>Article 3:</strong> The interception without right, by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.</td>
<td>163, 359, 362(2)</td>
</tr>
<tr>
<td>Data interference</td>
<td><strong>Article 4:</strong> The damaging, deletion, deterioration, alteration or suppression of computer data without right.</td>
<td>361 (1)</td>
</tr>
<tr>
<td>System interference</td>
<td><strong>Article 5:</strong> The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.</td>
<td>361 (1), 363-1</td>
</tr>
<tr>
<td>Misuse of devises</td>
<td><strong>Article 6 (b):</strong> The possession of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses; or a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing illegal access/illegal interception/data interference/system interference.</td>
<td>361-1</td>
</tr>
<tr>
<td>Computer-related forgery</td>
<td><strong>Article 7:</strong> The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible, committed intentionally and without right.</td>
<td>362 (1)</td>
</tr>
<tr>
<td>Computer-related fraud</td>
<td><strong>Article 8:</strong> The causing of a loss of property to another person by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</td>
<td>190 (3)</td>
</tr>
<tr>
<td>Offenses related to child pornography</td>
<td><strong>Article 9:</strong> The producing of child pornography for the purpose of its distribution through a computer system; the offering or making available child pornography through a computer system; the distributing or transmitting of child pornography through a computer system; the procuring of child pornography through a computer system for oneself or for another person; the possession of child pornography in a computer system or on a computer-data storage medium.</td>
<td>301</td>
</tr>
<tr>
<td>Offenses related to the infringements of copyright and related rights</td>
<td><strong>Article 10:</strong> The infringement of copyright as defined under the Paris Act of 24 July 1971, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty or the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention).</td>
<td>176</td>
</tr>
<tr>
<td>Corporate liability</td>
<td><strong>Article 12:</strong> The liability of legal persons for a criminal offense established in accordance with this Convention; committed for their benefit by any natural person; acting either individually or as part of an organ of the legal person, who has a leading position within it, based on power of representation of the legal person; or an authority to take decisions on behalf of the legal person; or an authority to exercise control within the legal person.</td>
<td>96</td>
</tr>
</tbody>
</table>
The second section of the second chapter prescribes the powers and procedures which shall be approved by the countries for the purpose of specific criminal investigations or proceedings.

**While Ukraine has mostly implemented the provisions of substantive law, the implementation of the procedural part is lacking important elements:**

1) The Code of Criminal Procedure does not contain the definition of electronic evidence which complicates the implementation of the substantive law. Ukraine can only accept as evidence electronic documents which should correspond to specific requirements. According to the Law on Electronic Documents and Documents Circulation, electronic documents shall be certified by electronic signature in order to prove authorship.

2) Obviously, files or other electronic traces are not signed with electronic signatures as it is difficult to imagine a hacker who will do such a thing purposefully. Thus, these files or traces may be not acceptable evidence in Ukrainian criminal courts. The prosecutor or investigator shall prove that such evidence is: 1) related to the case; 2) truthful; 3) enough to prove the fact; 4) obtained by legal means; 5) cannot be objected. This, in practice, creates difficulties to prove as the Code of Criminal Procedure does not identify the procedure for collecting evidence in electronic form and thus it is not clear what are the legal means for obtaining such evidence, their storage and protection from external influence. This leaves a window for judges’ decisions and discretion to consider the evidence as acceptable or not.

3) Enabling the collection of evidence in electronic form for a criminal offense will ensure the mutual assistance between signatories of the treaty to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data.

The Code of Criminal Procedure is lacking the definitions of subscriber, subscriber information, traffic data, and content data which creates difficulties with implementation. Ukraine also hasn’t implemented the provisions related to the expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data. The full implementation of the second section of the Budapest Convention on procedural law requires significant amendments to the Code of Criminal Procedure.

The third chapter of the Budapest Convention identifies the framework for international cooperation on counteracting cybercrimes. When it comes to international cooperation, the Budapest Convention recognizes extradition and mutual legal assistance. International cooperation in extradition is partly covered in Article 10 of the Criminal Code of Ukraine and bilateral agreements signed with different countries.

Cooperation with European Union countries is based on the Association Agreement between Ukraine, the European Union, the European Atomic Energy Community, and their Member States. The agreement was ratified by a statement in Law #1678-VII “On Ratification of the Association Agreement between Ukraine, the European Union, the European Atomic Energy Community, and their Member States. The agreement was ratified by a statement in Law #1678-VII “On Ratification of the Association Agreement between Ukraine,

---

9 Substantive law is the set of laws that governs how members of a society are to behave. It is contrasted with procedural law, which is the set of procedures for making, administering, and enforcing substantive law. Substantive law defines rights and responsibilities in civil law, and crimes and punishments in criminal law. It may be codified in statutes or exist through precedent in common law.

10 Expedited preservation of stored data, also known as 'quick freeze' or data preservation, refers to situations where a person or organization (which may be a communications service provider or any physical or legal person who has possession or control of the specified computer data) is required by a state authority to preserve specified data from loss or modification for a specific period of time (a maximum of 90 days under the Budapest Convention).
on the one hand, and the European Union, the European Atomic Energy Community and their Member States, on the other hand” on September 16, 2014. Ukraine has also signed bilateral agreements with more than 30 countries.

Ukraine identified the authorities responsible for mutual legal assistance. During the stage of pre-trial investigation, the Prosecutor General’s Office (Department for International Legal Cooperation and European Integration) is the central authority. At the trial stage, the Ministry of Justice (Division on Mutual Legal Assistance in Criminal Matters, International Legal Cooperation Department, Directorate for International Law) handles mutual assistance requests. In the absence of a treaty between countries, requests on mutual legal assistance should go through the Ministry of Foreign Affairs (Directorate General for Consular Service).

NIS Directive

On 6 July 2016, the European Parliament adopted the Directive on Security of Network and Information Systems (the NIS Directive) which is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU by ensuring effective operations of the Computer Security Incident Response Team (CSIRT or CERT) and competent network and information systems authorities, intensifying international cooperation, and establishing a culture of compliance with the security and notification requirements under the NIS Directive. The NIS Directive is supplemented by the NIS Toolkit – a Communication that aims to support EU-member states in their efforts to implement the NIS Directive swiftly and coherently across the EU. It presents best practices, explanation, and interpretation of the NIS Directive.

According to the NIS, Directive EU member countries shall fulfill certain obligations which Ukraine has already partly implemented:

<table>
<thead>
<tr>
<th>NIS Directive</th>
<th>Ukraine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adopt a national strategy on the security of network and information systems</td>
<td>Ukraine adopted a Cybersecurity Strategy in 2016. This strategy outlines threats to cyberspace, delineation of powers between state authorities responsible for cybersecurity, strategic objectives and priorities for national cybersecurity.</td>
</tr>
<tr>
<td>Create a cooperation group to support and facilitate strategic cooperation and the exchange of information among EU member states and to develop trust and confidence amongst them</td>
<td>Ukrainian cybersecurity authorities established contact with their peers in EU member states, actively cooperate with them and exchange information. According to the NIS Directive, each country shall establish a national cooperation group to support and facilitate strategic cooperation and exchange of information with other EU member states. However, there is no single formal cooperation group in Ukraine which would facilitate this and develop trust and confidence among EU member states.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NIS Directive</th>
<th>Ukraine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish security and notification requirements for operators of essential services and for digital service providers</td>
<td><strong>Ukraine</strong> made efforts to establish security requirements for the operators of essential services. Specifically, the Draft Law on CI and its protection was developed, as well as drafts of Cabinet of Ministers Resolutions which would set the requirements for the security of CI. The status and perspectives for adoption of these drafts are described in further chapters of this report. The Law on Cybersecurity obliges the operators of CI objects to inform CERT-UA on cyber incidents; however, as the legislation on CI is pending and there is no list of such objects yet, de facto this norm remains declarative. Cabinet of Ministers of Ukraine Resolution No. 518 of 19 June 2019 specified that the owner and/or CEO of a CI object must organize urgent notification of CERT-UA (if available, sectoral Computer Security Incident Response Team) as well as the functional unit for counterintelligence protection of state interests in the sphere of information security of the SSU Central Office (SSU Cybersecurity Situation Center) or respective unit of the regional SSU office on cyber incidents or cyberattacks involving its critical information infrastructure object of a CI object. However, the procedure and timeframe for such notifications are not established. Ukraine shall develop notification guidelines for CI operators on the circumstances in which they shall notify on incidents, the format, templates and procedure of such notifications, and the categorization of cyber incidents. Ukraine shall also establish the procedure of notification for EU member states on cyber incidents which may influence them. Also, it is not clear whether digital service providers will be assigned to the CI objects according to the legislation which may be adopted. In this regard, Ukraine shall develop the security and notification requirements for digital service providers.</td>
</tr>
<tr>
<td>Designate national competent authorities, single points of contact, and CSIRTs with tasks related to the security of network and information systems</td>
<td><strong>Due to the low-level of cooperation within Ukrainian authorities responsible for cybersecurity, it would be difficult to appoint a single point of contact, since this authority shall be responsible to coordinate and cooperate with Ukrainian authorities, liaise and ensure cross-border cooperation with other EU member states. Ukraine shall identify the national coordination authority which will be not just tasked but also able to coordinate the efforts of multiple national authorities.</strong></td>
</tr>
</tbody>
</table>
The SSSCIP is trying to introduce the NIS Directive requirements into the legislation they draft. However, their representatives have acknowledged that international assistance will be valuable while drafting comprehensive laws on cybersecurity which will comply with NIS Directive requirements.

Conclusions:

4) While there is no global comprehensive treaty regulating cybersecurity issues, the 2000 UN Convention Against Transnational Organized Crime and the 1992 Constitution of the International Telecommunication Union (which partly regulate cybersecurity issues at the global level), serve as guidelines for countries on how to improve security in cyberspace. These documents are supplemented in that regard by the 2015 United Nations Report on Cybersecurity. While certain treaties such as the 2000 UN Convention Against Transnational Organized Crime and 1992 Constitution of the International Telecommunication Union partly regulate cybersecurity issues at the global level, supplemented by the 2015 UN Report on Cybersecurity; serve as guidelines for countries on how to improve security in cyberspace, there is no global comprehensive treaty regulating cybersecurity issues;

• The Budapest Convention on Cybercrimes is the only regional binding document on cybersecurity. As a signatory to this convention, Ukraine has implemented most of the substantive legal provisions in domestic legislation. However, in order to implement all the provisions of the Budapest Convention effectively, the Code of Criminal Procedure of Ukraine needs to provide more comprehensive definitions to cybersecurity terminology;

• As Ukraine is not part of the EU, the NIS Directive is not binding; however, it serves as a guideline for good practice. While some of the provisions were voluntary implemented in Ukrainian legislation, others remain unaddressed

National Legislation

The Constitution of Ukraine in Article 17 states that information security is one of the most important functions of the state and a matter of concern for all Ukrainian people. Article 18 of the Constitution of Ukraine prescribes that the foreign political activity of Ukraine shall be aimed at ensuring its national interests and security by maintaining peaceful and mutually-beneficial cooperation with members of the international community in compliance with generally acknowledged principles and norms of international law.

According to Article 106 of the Constitution of Ukraine, the President plays an important role in ensuring national security which includes cybersecurity, specifically by presiding the National Security and Defense Council, leading the national security and defense, and proposing to Parliament the candidate for the Head of the Security Service of Ukraine or his/her discharge from office.

The National Security and Defense Council is the coordinating body to the President of Ukraine on issues of national security and defense. The President individually designates the membership of the National Security and Defense Council. The operations of the National Security and Defense Council are regulated by the Law on National Security and Defense Council which empowers it to consider issues identified by the National Security Strategy of Ukraine. As cybersecurity is one of the issues identified, the National Security and Defense Council adopted the Cybersecurity Strategy.
Cybersecurity Strategy

To implement the Budapest Convention, the National Security and Defense Council of Ukraine adopted a Resolution on the Cybersecurity Strategy of Ukraine, subsequently approved by an act of secondary legislation – Presidential Decree No. 96 of 15 March 2016 (the Cybersecurity Strategy)\(^{13}\). While there is no specific timeframe for implementation of the Cybersecurity Strategy, it references the Ukrainian National Security Strategy which expires in 2020. The strategy is supplemented by the annual Action Plans that was approved by the Cabinet of Ministers of Ukraine in 2016; however, the last Action Plan was adopted in 2018 and the plan for 2019, at the time of writing this report, has not yet been adopted. SSSCIP believes that the overall progress of the Cybersecurity Strategy implementation will be evaluated, as there is no reliable and comprehensive data on the progress of its implementation.

Cybersecurity strategy goals

The main goal of Ukraine’s National Cybersecurity Strategy is to create the conditions needed to ensure safe cyberspace and its use in the interests of individuals, society and the government. The Ukrainian National Security and Defense Council identified the following objectives to achieve the main goal:

1) Creating the national cybersecurity system;
2) Strengthening the capacity of cybersecurity stakeholders to counteract military cyberthreats, cyber-espionage, cyberterrorism, and cybercrimes, to deepen the international cooperation on cybersecurity; and
3) Ensuring cybersecurity of state electronic and informational systems and informational infrastructure under Ukrainian jurisdiction.

At the same time, the Cybersecurity Strategy does not specify how these goals will be achieved, leaving this for regulation by other acts.

Cyberthreats

The National Security and Defense Council acknowledges the importance of cyberspace and its vulnerability to external influence. It emphasizes the special gravity of cybersecurity for the military sphere, where usage of modern informational technologies has increased significantly due to the hybrid war with the Russian Federation. It also endorses the notion that CI objects could be targets of cyberterrorism, and that informational resources of financial institutions, transport and energy companies, state agencies responsible for emergency response frequently become an object for cyberattacks and cybercrimes.

Such vulnerabilities evolve into cyberthreats due to:

- Inadequate electronic communication infrastructure, its development and its protection in comparison to modern requirements; Insufficient and inconsistent CI protection;
- Insufficient development of organizational and technical infrastructure for ensuring cybersecurity and cyber protection of CI and state electronic informational resources;
- Lack of capacity by security and defense stakeholders to counteract cyberthreats of military, criminal and terrorist nature;
- Lack of coordination, cooperation and information exchange between cybersecurity agencies.

Cybersecurity priorities

The Cybersecurity Strategy of Ukraine identifies the following strategic priorities for the country:

- Development of safe, sustainable and reliable cyberspace
- Security of government information resources
- Security of CI
- Development of cybersecurity capacities in the defense sector
- Fighting cybercrimes

For each of the priorities, the Cybersecurity Strategy defines the directions for their implementation. In its report, MITRE assessed that Ukraine has established realistic strategic objectives in cyber and possesses the technical talent to achieve them if these advantages are leveraged by a commitment to change through focused, disciplined and collaborative efforts\[14]. At the same time, MITRE identified three primary risks to Ukraine’s strategic objectives that should be achieved:

1) Challenges in developing operational resilience sufficient to counter ongoing cyberthreats, including Russian aggression;
2) Fiscal constraints that limit the government’s ability to pay competitive wages to attract and retain the cybersecurity workforce they need; and
3) A policy and governance structure that needs greater intragovernmental coordination to develop consensus risk management and resourcing approaches, aligned with strategic priorities, to build strategic and operational resilience.

Delineation of powers between cybersecurity agencies

A number of stakeholders, including security, defense, communications, and police agencies of Ukraine, are tasked with implementing the Cybersecurity Strategy (See Annex B). At the same time, the Cybersecurity Strategy is a piece of secondary legislation and thus cannot be implemented directly by the state agencies, which according to Article 6 of Constitution of Ukraine shall execute their powers within and according to the laws of Ukraine. While some of these powers are organizational and mentioning them in the Strategy was done to make it clear who is responsible for what, others are rule-making and enforcement cannot be implemented without changes in the Laws on SSSCIP or SSU. In this regard, the Cybersecurity Strategy serves more as a guideline for further implementation in primary legislation than as an act of direct power.

At the same time, the Cybersecurity Strategy does not set up an effective mechanism for intergovernmental cooperation. According to the Strategy, the National Security and Defense Council of Ukraine and its National Cybersecurity Coordination Centre are assigned to coordinate and control activities of security and defense in the field; this complies with Article 107 of the Constitution of Ukraine. Assigning powers to the state agencies goes beyond the authority of the President and the National Security and Defense Council, as according to the Constitution such powers can be determined only by the laws. At the same time, MITRE’s report from 20 January 2018.

---

\[14\] Ukraine National Cybersecurity Strategy Assessment and Recommendations, MITRE’s report from 20 January 2018.
time, the National Security and Defense Council lacks the capacity to coordinate and control security and defense cybersecurity activities. It does not have enough qualified personnel able to coordinate the efforts of the SSSCIP or SSU. In practice, such coordination is conducted through occasional meetings which are usually scheduled only in case of emergency or serious threats. There is no regular coordination and information sharing, nor does any authority have the full understanding of the situation. Each agency is acting according to its own priorities and within their own mandate, and coordinates efforts with other agencies on an ad hoc basis. To address this, an information sharing hub shall be established. For example, in the US model an Information Sharing and Analysis Center serves as a hub for sharing information between the cybersecurity agencies.

The Office of the newly-elected President of Ukraine Volodymyr Zelenskyi identified digitalization as one of its key priorities. In particular, this also influenced the work of the National Defense and Security Council, which on 1 August 2019 created a Working Group on Reforming Cybersecurity within the System of National Security of Ukraine. One positive point worthy of mention here is that the Group includes a number of recognized cybersecurity experts from private cybersecurity companies. On 27 June 2019 the Secretary of the National Defense and Security Council announced that an updated Cybersecurity Strategy will be adopted in Ukraine. Such strategy will be developed based on the results of reviewing the state of cybersecurity of electronic information resources. At present, however, it is not known who will perform such a review, and how.

**Primary Legislation Level. Law on Cybersecurity**

The legislative framework on cybersecurity in Ukraine includes:

- Law No. 2229-XII of 25 March 1992 on Security Service of Ukraine;
- Law No. 2135-XII of 18 February 1992 on Counterintelligence Activity;
- Law No. 3475-IV of 23 February 2006 on Ukraine State Service of Special Communication and Information Protection;
- Law No. 1280-IV of 18 November 2003 on Telecommunications; Law No. 3855-XII of 21 January 1994 on State Secrets;
- Law No. 2297-VI of 1 June 2010 on Personal Data Protection;
- Law No. 2469-VIII of 21 June 2018 on National Security of Ukraine;
- Law No. 851-IV of 22 May 2003 on Electronic Documents and Electronic Document Circulation
- Law No. 3341-XII of 30 June 1993 on Organizational and Legal Framework on Fight against Organized Crime; and

On October 5, 2017, the Ukrainian Parliament passed Law No 2163-VIII on the Main Principles of Maintaining Cybersecurity of Ukraine – a framework piece of legislation that needs to be specified in the secondary legislation.

In general, the process of preparing and adopting the Law on Cybersecurity lacked transparency and inclusivity; therefore, many provisions face resistance from stakeholders. As mentioned earlier, many
stakeholders believe that the development of a comprehensive law to regulate cybersecurity issues is needed, while the current Law on Cybersecurity serves as a declaration of intentions and strategy.

The Law on Cybersecurity was adopted as a result of the Cybersecurity Strategy, aiming to identify the framework for the reform of the cybersecurity system of Ukraine. The Law on Cybersecurity defines the important terminology; lays down the main directions of state policy on cybersecurity, as well as the roles of the major responsible stakeholders; and introduces the concept of CI, mandating stringent security requirements for organizations running CI.

For the first time, the Law on Cybersecurity has identified the following terms in the Ukrainian legal syntax: cybersecurity, cyberthreat, cyberspace, cyber incident, cyberespionage, cyberterrorism. Previously, Ukraine had avoided using the term “cyber” in its legal framework and mostly used “information” or “electronic” to regulate issues related to cybersecurity. While the Cybersecurity Strategy mentions many “cyber” terms, it does not define those terms. At the same time, new terms do not correspond to the terms which were previously used in other laws. In this regard, legislation should be reviewed to harmonize with newly adopted Law on Cybersecurity. Moreover, the language explaining new terminology requires further clarification.

The Law on Cybersecurity does not apply to: 1) the content of the information being processed in communication and/or technological systems; 2) activities related to securing information classified as state secrets as well as the systems which process this information; 3) social media and private networks (if they do not contain information which should be protected according to the law), including blog platforms, video hosting and other web resources and services related to their functioning; and 4) communication systems which are not connected to the Internet or public networks (except technological systems).

The Law on Cybersecurity prescribes that the Cabinet of Ministers shall list CI and maintain its register, but the law does not specify the criteria for assigning objects to CI or the principles and procedures of maintaining their register, leaving these issues for regulation through secondary legislation. This also opens a window for political manipulation, especially when designating private entity systems as CI. Regulating these issues at the primary legislation level will guarantee its legal certainty, as passing laws requires consensus within Parliament and can prevent situations where the criteria or procedure by which systems are designated as CI can be easily changed by politically-motivated government decisions. It also makes amendment of such regulations less flexible, as laws need to be adopted by 226 votes and promulgated by the president.

According to the Law on Cybersecurity, the operators of CI shall inform CERT-UA about cyber incidents; but in the absence of CI regulation this norm remains declarative. The law defines that the Cabinet of Ministers of Ukraine shall adopt relevant by-laws regulating the designation of CI, the auditing procedure, and requirements for their security. The process of development and approval of such by-laws is described later in this report. According to the law, SSSCIP is responsible for auditing CI including the certification of auditors. Some stakeholders raised concerns about the risk of corruption associated with this function.

Complementing the Cybersecurity Strategy, the Law on Cybersecurity similarly identifies the roles and powers of cybersecurity authorities and stakeholders. At the same time, as the Cybersecurity Strategy does not specify how these powers shall be implemented; this leads to a situation in which several authorities are responsible for the same activities. In practice, it means that no authority takes responsibility. For example, both the SSSCIP and the SSU are responsible for reacting to cyber incidents, except that the
SSSCIP is responsible for all cyber incidents and the SSU only for cyber incidents that impact state security. In practice, this is not a distinction that is easy to make, and it often comes down to the discretion of the SSU staff.

The law strengthens the powers of the SSU, which is empowered to check the preparedness of CI to protect against cyber incidents and cyberattacks secretly. The law does not define the procedure for such checking. Many stakeholders raised serious concerns about the extension of SSU powers. Such empowering of the SSU could lead to unlawful interference of the SSU in commercial activities or arbitrary access to personal data.

The paths of public-private partnership are defined by the law and include:

- Involving volunteer organizations in detecting and counteracting cybercrimes;
- Increasing public awareness on cybersecurity; Exchanging information on cyberthreats to CI;
- Cooperation of CERT-UA with other computer emergency response teams; Engaging experts and academics in the development of key sectoral legal drafts;
- Providing consultative and practical assistance for responding to cyberattacks;
- Establishing consultative centers for citizens and representatives of business on ensuring cybersecurity;
- Conducting periodic national summits with professional business service providers, including insurers, auditors, lawyers, identifying their role in promoting better risk management in cybersecurity;
- Building a system of training and strengthening the capacity of cybersecurity experts; and
- Cooperation with private persons, NGOs and IT companies on ensuring cyber defense in cyberspace.

While all these paths are important, and the effectiveness of cybersecurity would benefit from public-private partnership, in practice this norm remains declarative. Representatives of the SSSCIP acknowledged that private companies are not eager to cooperate with the state authorities predominantly because they do not see the benefits of such cooperation.

Importantly, the Law allows cybersecurity subjects to cooperate internationally with their peers from other countries based on bilateral or multilateral agreements. The Law on Cybersecurity also establishes the requirement to conduct an independent audit of cybersecurity effectiveness; however, it does not specify who should conduct such audit and how, who should initiate it, or how it will comply with state security requirements. Furthermore, the law does not define who should establish the auditing procedure. Without changing the Law on Cybersecurity to specify this, such provisions will remain declarative.

Eight bills regulating some aspects of cybersecurity were registered at the Parliament’s 8th convocation (see Annex A) aiming to:

- Delineate the jurisdiction of the investigation of crimes committed in the use of electronic computing machines (computers), systems, computer networks and telecommunication networks, state information resources and CI;
- Establish or strengthen the liability for cyberterrorism and cybercrime;
- Strengthen the liability for offenses committed in the sphere of information security and combating cybercrimes;
- Counteract threats to national security in the information sphere.
Pursuant to the Verkhovna Rada Rules of Procedure, draft laws that were not considered in the first reading by the Parliament during its 8th convocation are deemed to have been dismissed; they can be considered later only if they are submitted to the Verkhovna Rada’s 9th convocation by holders of the right to legislative initiative.

At present, only one bill related to regulation of certain cybersecurity aspects is registered at the Parliament: Draft Law No. 2043 of 3 September 2019 “On Amending the Law of Ukraine ‘On Protection of Information in Information and Telecommunication Systems’ (Regarding Confirmation of Information System Conformity to Information Protection Requirements)”15. This draft was submitted by MPs from the ruling Servant of the People party – Mykhailo Kriachko and Oleksandr Fedienko, which means that it is highly likely that the Parliament will support it. The draft is being processed at the Committee on Digital Transformation. If it is adopted, then, in respect of open and confidential information which is legally required to be protected or which belongs to state information resources, there will be an alternative procedure for confirming information system conformity to information protection requirements, which will not require the creation of a comprehensive information protection system.

System conformity to information protection requirements will be deemed confirmed if the following set of conditions is met:

- Confirmation of conformity of the information security management system based on the results of a conformity assessment procedure performed in the manner prescribed by the law, having regard to sectoral requirements and information security norms;
- Use for protection of information within a system of instruments with confirmed conformity in the sphere of technical and/or cryptographic protection of information;
- Placement of all system elements within territories under Ukrainian control.

Undoubtedly, the adoption of such a draft law will simplify the work of state bodies and reduce unnecessary bureaucratic workload. The draft has been developed in line with the Concept of the National Program for Adaptation of the Legislation of Ukraine to the Legislation of the European Union, which was approved by Law of Ukraine № 228-IV of 21 November 2002. It will contribute to the approximation of Ukrainian legislation to EU legislation and the creation of a legal framework for Ukraine’s integration in the European Union.

Secondary Legislation Level

Secondary legislation under the Law of Cybersecurity should have been approved within 3 months from its entry into force of law; however, the Cabinet of Ministers has failed do so. SSSCIP has developed drafts of the Cabinet of Ministers Resolutions related to the CI protection; the status of these drafts will be analyzed in the chapter on CI.

At the same time, several important matters are regulated at the secondary legislation level legislation level:

- President’s Decree No. 96 of 15 March 2016 on the decision of the National Security and Defense;

• President’s Decree No. 505/98 of 22 May 1998 on Regulation Procedure for the Implementation of Cryptographic Information Security in Ukraine;

• President’s Decree No. 1229/99 of 27 September 1999 on Regulation on Technical Protection of Information in Ukraine;

• President’s Decree No. 184/2015 of 30 March 2015 on the decision of the Council of National Security and Defense of Ukraine dated March 12, 2015 “On the Status of Overcoming the Negative Consequences Caused by the Loss of Material Carriers of Classified Information in the Temporarily Occupied Territory of Ukraine in the Area of Anti-terrorist Operation in the Donetsk and Luhansk Oblasts» (classified, publicly not available);

• President’s Decree No. 32/2017 of 13 February 2017 “On the decision of the National Security and Defense Council of Ukraine dated 29 December 2016 ‘On State Cyberthreats and Urgent Measures to Neutralize Them”;

• Cabinet of Ministers of Ukraine Resolution No. 1519 of 11 October 2002 “On Approval of the Procedure for Providing Confidential Communication Services to State Authorities and Local Self-Government Bodies, State Enterprises, Institutions and Organizations;

• Cabinet of Ministers of Ukraine Resolution No. 303 of 14 May 2015 “Some Questions of Organization of Interagency Information Exchange in the National System of Confidential Communication” Cabinet of Ministers of Ukraine Order No. 1009 of 06 December 2017 “On Approval of the Concept of State System for CI Protection”.

Conclusions:

• In recent years, Ukraine has adopted a number of acts governing cybersecurity issues which constitute its national legal framework on cybersecurity;

• Adopted in 2016, Ukraine’s National Cybersecurity Strategy is an act of secondary legislation which identifies the goals and priorities for cybersecurity until 2020. Its provisions were further implemented in the Law on Cybersecurity adopted in 2017. The latter identifies important terms, delineates powers between cybersecurity agencies and defines the principles of further regulation of CI protection and public-private partnerships;

• The Law on Cybersecurity is a fairly high-level framework set of rules and requirements; it does not go into much detail, leaving it to be addressed by the secondary legislation, to be approved by the Cabinet of Ministers of Ukraine. While the deadline for adopting such acts already passed in August 2018, the drafts which were developed by the SSSCIP are still under the consideration of the Cabinet of Ministers and chances for their adoption in the nearest future are low. Without such acts of secondary legislation, many provisions of the law remain declarative;

• As different laws governing cybersecurity were adopted at different times, the usage of terminology is inconsistent and there is no clarity in the delineation of powers between cybersecurity agencies.
Regulation on Critical Infrastructure Protection

Ukrainian authorities do not have a clear vision of how to regulate issues of CI protection\textsuperscript{16}. On the one hand, the Cabinet of Ministers of Ukraine approved the Concept for Creating a State System for the Protection of Critical Infrastructure (hereinafter, the Concept of CI Protection) on December 6, 2017, just two months after the adoption of the new Law on Cybersecurity\textsuperscript{17}. While the newly-adopted Law on Cybersecurity provides for the regulation of CI protection at the secondary legislative level through Cabinet of Ministers Resolutions, the Concept of CI Protection envisions the development and approval of a separate law on CI protection – to regulate the issue at the primary legislation level. On the other hand, the provisions of the Law on Cybersecurity which oblige the Cabinet of Ministers to approve by-laws are still in place and relevant.

The Cabinet of Ministers has been considering both options for regulating CI protection – at the primary or secondary legislation levels\textsuperscript{18}. Meanwhile, the Cabinet of Ministers adopted a Concept of CI protection which describes how future regulations of this issue should look.

Concept of Critical Infrastructure Protection

The Concept of CI Protection was adopted by the Cabinet of Ministers of Ukraine on the implementation of UN Resolution #2341 of 13 February 2017, “The Protection of CI Against Terrorist Attacks,” which had been initiated by Ukraine. The Concept of CI Protection is aimed to determine the main directions, mechanisms and terms of the complex legal regulation of CI protection and the establishment of an appropriate public administration system. The implementation period of the Concept of CI Protection is 10 years (until 2027). The Concept of CI protection envisions legislative, institutional and organizational changes to the existing system of CI protection.

In the Concept of CI Protection, the Cabinet of Ministers acknowledged the existence of gaps and inconsistencies in the current legislation regulating CI protection, including:

- The lack of a special law on CI protection;
- The absence of a unified nationwide system of CI protection and special authority to coordinate actions for CI protection;
- The uncertainty of powers, tasks, and responsibilities of authorities responsible for CI protection;
- The omission of common criteria for designating CI;
- The dearth of procedure of CI certification and categorization; and
- The lack of unified methodology for assessing threats to CI and special authority responsible for its conduction.

\textsuperscript{16} According to Article 6 of Law on Cybersecurity, critical infrastructure is enterprises, institutions and organizations irrespective of ownership, whose activities are directly related to technological processes and/or providing services of major importance to the economy and industry, the functioning of the society and the safety of the population, the failure or disruption of which may have a negative impact on the state of national security and defense of Ukraine, the environment, property and/or human life and health.

\textsuperscript{17} https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritchnoiy-infrastrukturi.

\textsuperscript{18} Information confirmed by the SSSCIP representatives.
The Cabinet of Ministers also recognized the weakness of public-private partnership in the field of CI protection and insufficient international cooperation in this sphere.

**Draft Law on Critical Infrastructure Protection**

The Draft Law on Critical Infrastructure and Its Protection was developed as a result of approval of the Concept of CI Protection by the working group at the Ministry of Economic Development and Trade with the involvement of key agencies responsible for cybersecurity. Though some Ministries and agencies expressed serious concern about the content of the draft law prepared by the Cabinet of Ministers, on 27 May 2019 it was registered at the Verkhovna Rada; it was not considered before the termination of the mandate of the Verkhovna Rada of the 8th convocation and hence it is deemed to have been withdrawn.

At the same time, the registration of the Draft Law on CI and Its Protection was preceded by considerable work, and its provisions can thus be used as a basis for a draft law that will be developed in the future. Therefore it deserved to be analyzed separately, with identification of its strengths and attention to essential faults that should be taken into account in subsequent work.

The Draft Law on CI and Its Protection does the following:

1) Provides a number of important definitions: CI; act of unauthorized interference; CI security; state systems under CI protection; vital services; vital functions; CI protection; classification of infrastructure criticality; categorization of infrastructure objects; crisis situation; CI objects; CI operator; protection of CI; security passport; level of criticality; CI operating mode; CI sector; CI stability; actors of the state system of CI protection; and critical technological information;

Many stakeholders raised concerns that terminology used in the draft does not correspond to the terminology of other legislation; there is a need for a comprehensive legal analysis of the terms used in different laws and drafts so they are consistent. Additionally, some of the terms are explained with words requiring additional explanation. For instance, the draft defines CI objects as an integral part of CI, the functionality, continuity, integrity and stability of which ensure the implementation of vital national interests. However, the draft does not stipulate what the vital national interests are which may cause difficulties in its implementation.

2) Identifies the main principles, goals and tasks of the state policy on CI protection;

3) Assigns to the CI any enterprises, institutions, organizations irrespective of the form of ownership which are:

   a. carrying out activities and providing services in the fields of energy; chemical industry;
   b. transportation; information and communication technologies; electronic communications; and banking and financial sectors;
   c. providing services in life support, centralized water supply, centralized drainage, energy, hot water, electric energy and gas, food production, food services, and health care;

---

19 [http://www.me.gov.ua/Documents/Download?id=634a8762-3d1a-45ac-b0df-be56a4f7d9d1](http://www.me.gov.ua/Documents/Download?id=634a8762-3d1a-45ac-b0df-be56a4f7d9d1).
21 According to the Rules of Procedure of the Verkhovna Rada, all the drafts which were registered within the mandate of the current composition of the Verkhovna Rada will be annulled and will have to be registered again within the mandate of the next composition of Verkhovna Rada to be considered.
d. included in the list of enterprises of strategic importance to the economy and security of the state;

e. subject to protection and defense in a state of emergency and a special period; objects or assets representing a high danger;

f. objects or assets of national importance, objects which have branched links and significant influence on other infrastructure; and

g. objects or assets the disruption of which would lead to a crisis of regional importance;

4) Determines the criteria for designating what CI is;

However, the draft does not define the methodology for assessing threats to CI or reacting to them as prescribed by the Cybersecurity Strategy;

5) Defines four categories of criticality and authorities responsible for assigning CI objects to certain categories;

The Cabinet of Ministers is planning to delegate the authority for CI identification and risk assessment to each responsible ministry or agency; this will not contribute to the consistency of such assessments, especially in the absence of a clear methodology.

6) Identifies the procedure for creating and maintaining the National List of CI Objects and the procedure for CI objects certification;

7) Appoints the Cabinet of Ministers as coordinator of efforts on CI protection. An Authorized Agency for Critical Infrastructure Protection shall be established to form and implement state policy on CI protection;

Civil society organizations raised concerns about the absence of a procedure for the establishment of an authority with such significant power22. As CI is a broad phenomenon which may involve entities from different sectors, such an entity would need to have the authority to coordinate many different stakeholders with contrasting interests;

8) Identifies the powers of agencies responsible for CI protection, empowers SSU with a wide authority on CI protection and SSSCIP with wide authority on critical information infrastructure protection.

The Internet Association of Ukraine criticized this approach, arguing that SSU already has enough powers prescribed by the Special Law on SSU to protect CI23. Moreover, as the draft does not define the procedure for executing SSU’s new power, it would, on the one hand, complicate implementation of the law, and on the other hand, provide SSU with unlimited discretion. Civil society organizations (CSOs) also raised concerns about the potential extension of SSU power to restrict and block access to facilities and resources used for organizing, committing, funding, facilitating or concealing an act of unauthorized interference into the operation of CI, as this may include blocking websites, which contradicts Council of Europe recommendations24. This also contradicts Article 4.5 of the Cybersecurity

24  Recommendations of the Council of Europe CM/Rec (2016)5 on Internet freedom state that restricting access to websites shall be based on a decision of a court or other independent administrative body that is subject to judicial review.
Strategy which defines that blocking informational resources can be done only by court decision. The draft also entitles SSU to check all service provider contracts for CI without specifying the subject of such contracts and the procedure for checking them. As such, this power is vulnerable to abuse. At the same time, some CSOs argue that the draft does not define the authorities for non-state (private and local administrative level) protection for CI objects;

9) Establishes the cybersecurity responsibilities of CI operators. This draft provision has been harshly criticized, as it fails to define the sources of funding needed for introducing cybersecurity measures or the compensation from the state; and

10) Determines the way of public-private cooperation on CI protection and principles of international cooperation in this area.

The State Regulatory Service of Ukraine refused to approve the draft, arguing that the drafters have not: calculated budgetary assignments which should be allocated for the implementation of the law; described the alternative approaches; evaluated the percentage of each group of business entities which will be influenced by adoption of the law; or specified the time and material resources necessary from CI operators to ensure cybersecurity measure prescribed by the draft.\(^{25}\)

The draft law was not considered before the end of the mandate of the Verkhovna Rada of Ukraine of the 8th convocation; therefore, at the beginning of the Parliament’s new convocation it is deemed to have been withdrawn. At present, it is not clear whether the new authorities of Ukraine will use this draft as a basis when developing legislation on CI protection or whether they will get back to the drawing board. One thing is clear: Ukraine urgently needs legislation regulating CI protection.

**Drafts of Secondary Legislation**

SSSCIP has developed three drafts of Cabinet of Ministers’ Resolutions on the audit of CI objects, forming a list of CI objects, recording CI objects in the National Register, the criteria and procedure for assigning objects to CI, and general cybersecurity requirements for such objects (see Annex A). These drafts were developed by SSSCIP’s Department of Development and Implementation of State Policy on Cybersecurity under the provisions of the Law on Cybersecurity.

While the Law on Cybersecurity stipulates that the Cabinet of Ministers should have adopted secondary legislation within three months of entry into force of the law, the process of coordinating drafts with relevant ministries and agencies is complicated and bureaucratic. The drafts were developed, published on the SSSCIP’s website for public discussion and sent to the relevant institutions for their feedback. After receiving input from the relevant stakeholders, the SSSCIP adjusted the drafts and published them again for public discussion; in some cases SSSCIP had to publish 3rd and 4th versions of the initial drafts. According to the SSSCIP, the drafts were approved by all relevant ministries and agencies and are ready to be considered at a meeting of the Cabinet of Ministers.

However, the SSSCIP found that recent changes of procedure require approval from one more agency. According to Paragraph 33.5 of the Cabinet of Ministers’ Rules of Procedure, drafts related to the informatization, formation and usage of national electronic informational resources shall be coordinated with the State Agency for E-governance of Ukraine which shall conduct digital expertise of such resources.

drafts\textsuperscript{26}. Thus, the SSSCIP sent the drafts to the State Agency for E-governance of Ukraine which has its own recommendations for improvement and SSSCIP is ready to adjust the drafts according to these recommendations. However, SSSCIP is not certain whether or not the adjusted drafts should be published for public discussion once again. As this new regulation was introduced at the end of January 2019, there is no practice on its implementation yet and the provisions of the Cabinet of Ministers’ Rules of Procedure are unclear.

In the final weeks of the functioning of former Prime Minister Volodymyr Groysman’s Cabinet, on 19 June 2019, Cabinet of Ministers of Ukraine by Resolution No. 518 approved the General Requirements Regarding Cybersecurity of Critical Infrastructure Objects which define the organizational, methodological, technical and technological conditions for cybersecurity of CI objects that are binding on enterprises, institutions and organizations which are assigned by legislation to critical infrastructure objects. The General Requirements provide, inter alia, for the obligation of the owner and/or CEO of a CI object to organize urgent notification of CERT-UA (if available, sectoral Computer Security Incident Response Team) as well as the functional unit for counterintelligence protection of state interests in the sphere of information security of the SSU Central Office (SSU Cybersecurity Situation Center) or respective unit of the regional SSU office on cyber incidents or cyberattacks involving its critical information infrastructure object of a CI object. However, the procedure and timeframe for such notification are not established.

Until the end of its mandate, however, Groysman’s Government did not approve the draft resolutions developed by SSSCIP on audits of CI objects, formation of a list of CI objects and entry of CI objects in the National Register or the criteria and procedure for assigning objects to CI. At present, it is not known for certain whether the new Government led by current Prime Minister Oleksiy Honcharuk will rely on what has been developed by his predecessors. The change of the SSU leadership and the potentially possible change of the leadership of SSSCIP do not make it more likely that these drafts will in fact be considered by Ukraine’s new Government.

**Conclusions:**

- Ukrainian authorities are not certain how to regulate issues of CI protection and are considering two options – to regulate it at the primary or secondary legislation level;
- Despite the fact that the Law on Cybersecurity prescribes the Cabinet of Ministers to adopt by-laws regulating criteria for assigning objects to CI, their audit, certification and cybersecurity requirements, the Cabinet of Ministers adopted the Concept of CI Protection, which envisions regulating this issue at the primary legislation level;
- As per the Concept of CI Protection, the Ministry of Economic Development and Trade developed the draft Law on CI and Its Protection, which was published for discussion in 2018. Many stakeholders agreed that the draft requires significant improvement. The Ministry of Economic Development and Trade adjusted the draft; it was registered at the Verkhovna Rada of 8th convocation and was not considered before the termination of its mandate; hence it is deemed rejected. It is not known at present when the Ukrainian authorities will get back to considering CI protection;
- Concurrently, SSSCIP developed drafts for secondary legislation regulating CI protection issues, but chances for their approval in the next half a year are similarly low.

\textsuperscript{26} https://zakon.rada.gov.ua/laws/show/950-2007-%D0%BF.
Gaps and Ambiguities of the Current Legislation

The weakness of the current provisions related to the cybersecurity regulation can be largely explained by the lack of a comprehensive legal framework and the existence of a number of gaps and ambiguities in the legislation. Among them:

- **The necessity to adjust domestic legislation in line with international commitments.** The Code of Criminal Procedure of Ukraine does not define the terms “subscriber”, “traffic data”, or “electronic evidence” and does not regulate the expedited preservation of stored computer data, the expedited preservation or partial disclosure of traffic data; this prevents Ukraine from effectively implementing other provisions of the Budapest Convention and limits the possibility for mutual assistance with other countries on prevention and counteraction of cybercrimes.

- **Inconsistency in terminology.** The Law on Cybersecurity defines a number of new terms; however, some of them do not correspond to the terms which were previously used in other laws. In this regard, earlier legislation should be reviewed to harmonize it with the newly adopted Law on Cybersecurity. Moreover, the language explaining new terminology is quite complicated itself and some wording requires further clarification.

- **The lack of regulation on critical infrastructure.** There lacks a single national system of protection for CI, and there is insufficient and inconsistent regulatory regulation on the protection of CI, in particular the absence of a special law on CI and its protection. The existing Resolution of the Cabinet of Ministers of Ukraine on the procedure for the formation of the list of information and telecommunication systems of state CI objects was approved in 2016, before the adoption of the Law on Cybersecurity, and contradicts the latter. The government failed to adopt the new regulation within the legal deadline prescribed by the Law on Cybersecurity, which passed in August 2018. Meanwhile, there is a lack of common criteria and methodology for designating infrastructure objects as CI, as well as the procedure of CI certification and categorization. As a result, the list of CI objects has not been approved yet and the provisions in the Law on Cybersecurity on the protection of CI remain declarative.

- **The absence of regulation for an information security audit of CI objects.** The new Law on Cybersecurity stipulates that the government shall adopt the regulations on requirements and procedures for the information security audit of the objects of CI. Such regulations should be based on international standards, including those of the European Union and NATO, developed with the mandatory involvement of representatives of the main national cybersecurity stakeholders, scientific institutions, independent auditors, experts in the field of cybersecurity, and NGOs. While the legal deadline passed in August 2018, the Cabinet of Minister failed to adopt such regulation.

- **The jurisdictional overlap.** The main authorities responsible for overseeing cybersecurity in Ukraine include the Ministry of Defense of Ukraine, the SSSCIP, the SSU, the National Police of Ukraine, the
National Bank of Ukraine, and intelligence agencies\textsuperscript{27}. There is a legal uncertainty of powers, tasks and duties of state agencies responsible for the protection of CI, as well as the rights and burdens of owners (managers) of CI objects. For example, the SSU and the Ministry of Internal Affairs have nearly identical mandates for cybersecurity investigation forensics, and no criteria exists with regard to allocation of work and tasks between these two institutions. While the Law on Cybersecurity assigned the responsibility for handling cyber incidents against CI to the SSU, this is not appropriately reflected in other relevant laws and regulations. Law enforcement powers such as those addressed in the Budapest Convention are not clearly defined under Ukrainian criminal procedure law, and this adversely affects law enforcement service provider cooperation, confidentiality rights and sometimes the rule of law.

- **The absence of security and notification requirements for operators of CI objects and digital service providers.** The NIS Directive requires countries to establish security and notification requirements for operators of essential services and for digital service providers. The Law on Cybersecurity requires operators of CI objects to inform CERT-UA about cyber incidents; however, as legislation on CI is pending and there is no list of such objects yet, this norm remains declarative de facto. Cabinet of Ministers of Ukraine by Resolution No. 518 of 19 June 2019 specified that the owner and/or CEO of a CI object must organize urgent notification of CERT-UA (if available, sectoral Computer Security Incident Response Team) as well as the functional unit for counterintelligence protection of state interests in the sphere of information security of the SSU Central Office (SSU Cybersecurity Situation Center) or respective unit of the regional SSU office on cyber incidents or cyberattacks involving its critical information infrastructure object of a CI object. However, the procedure and timeframe for such notification are not established. Ukraine shall develop the notification guidelines for CI operators about the circumstances under which they shall provide notification about incidents, the format, templates and procedure of such notification; and the categorization of cyber incidents. Ukraine shall also establish a procedure of notification to other states about cyber incidents which may influence them, bearing in mind confidentiality and commercial secret requirements. Also, it is not clear whether digital service providers would be assigned as CI according to the legislation yet to be adopted. As a result, Ukraine may have to develop security and notification requirements for digital service providers as well.

- **The lack of a Cybersecurity Strategic Plan.** In 2016 Ukraine approved a National Cybersecurity Strategy that identifies the main principles and goals for ensuring cybersecurity in Ukraine. Each year the government approves an annual action plan which defines activities for the year; however, the last action plan was adopted in 2018 and the plan for 2019 has not yet been adopted. At the same time, the process is lacking long-term strategic planning with clearly identified milestones, timeframes and responsibilities for their achievements. Development of the Strategic Plan will provide all stakeholders with an understanding of the main objectives, and how, when, by which

\textsuperscript{27} According to the Law on Intelligence Activity, the following authorities are entitled to conduct intelligence (investigative) activity: criminal and special police, State Bureau of Investigation, SSU, Foreign Intelligence Services of Ukraine, State Border Guard Service of Ukraine, Department of State Security, imprisonment and detention facilities, Ministry of Defense, National Anticorruption Bureau. The Law on Cybersecurity specifies which authorities are entitled to conduct intelligence; but it does not specify which ones are entitled to conduct intelligence activity on cybercrimes, leaving this norm blanket. This means that theoretically any of such authority may conduct intelligence activity on cybercrimes, although they might not be empowered for dealing with cybercrimes. Once again, such approach causes uncertainty at implementation level, where several authorities may feel that they are responsible for conducting intelligence activity or none feels the responsibility to conduct such activity.
means and by whom they will be achieved.

- **Fiscal constraints that limit the government’s ability to pay competitive wages to attract and retain the cybersecurity workforce they need.** In its report, MITRE highlighted the low salaries the government pays to the IT and cybersecurity personnel, which are much lower than salaries in the private sector. Many Ukrainian stakeholders agree that this is a constraint. The government is limited by legal requirements which should be changed to allow agencies to keep and motivate IT and cybersecurity staff. Moreover, low salaries increase the risk of insiders’ attacks and pose, by themselves, a cybersecurity vulnerability.

**Roadmap for Reforming Cybersecurity Legal Framework**

Over the past several years, Ukraine has taken a number of positive steps to implement its international commitments and improve legislation on cybersecurity; however, much effort is still needed. Initial recommendations for improvements include:

1. **Adoption of a comprehensive law on cybersecurity.** Adopted in 2017, the Law on Cybersecurity is a roadmap for future regulations. Bearing in mind the Ukrainian legal system and practice, Ukraine would benefit from approving a comprehensive law on cybersecurity in accordance with international standards and best practices that would regulate the full scale of cybersecurity issues. Adoption of such a law requires broad consultations with various stakeholders and the involvement of experts from different fields, including representatives of cybersecurity agencies, in its drafting, to address the complexity of the topic.

2. **All-inclusive review of cybersecurity legal framework in compliance with NIS Directive.** Ukraine requires a comprehensive review of primary and secondary legislation, identification of norms which contradict the NIS Directive, and proposal of amendments in accordance with the recommendations of the review. Ukrainian authorities lack the capacity to develop relevant drafts of legislation in accordance with NIS Directive requirements and require international assistance.

3. **Comprehensive review of legislation for consistency of cybersecurity terminology.** Different laws regulating cybersecurity were adopted at different times and use different terminology. This significantly complicates the process of their implementation. A comprehensive review of the terminology and harmonization of national legislation is needed to ensure a common understanding of cybersecurity.

4. **Development of strategic internal communication regarding cyber incidents.** The NIS Directive requires countries to establish security and communication protocols for operators of essential services and digital service providers. Information sharing about cyber incidents among CI stakeholders and cybersecurity agencies plays an important role in cybersecurity and approval of such requirements contribute to its effectiveness.

5. **Adoption of the Law on CI and relevant secondary legislation.** The Law on Cybersecurity and the Concept of CI Protection serve as a good start for the adoption of legislation governing CI protection. The adoption of secondary legislation could be considered a temporary option; however, there is a risk that operators of CI will not implement it properly.

6. **Adoption of the Law on Public-Private Partnership on Cybersecurity.** The Law on Cybersecurity
identifies the paths for public-private partnership; however, it does not define the mechanism for its implementation. The current Law on Public-Private Partnership focuses only on economic partnership and does not serve as an effective mechanism for public-private partnership in the cybersecurity field.

7. **Comprehensive review and amending laws on law enforcement agencies responsible for cybersecurity protection against cybercrimes and cyberterrorism.** Ukrainian cybersecurity stakeholders see the role and the powers of cybersecurity agencies and the process of assigning such powers differently. Because the Law on Cybersecurity assigned significant powers to the SSU and SSSCIP, many representatives of the private sector and NGOs complained that this was done in the Law on Cybersecurity instead of amending laws on SSU and SSSCIP. At the same time, the SSU and SSSCIP argue over a lack of powers and resources to work effectively. Ukraine will benefit from careful review and consultations on the delineation of powers between law enforcement agencies responsible for cybersecurity protection.

8. **Assessment of Cybersecurity Strategy Implementation.** The Cybersecurity Strategy was adopted in 2016 and since then there has been no evaluation of its implementation. As the strategy itself does not define measures and tools for assessing its effectiveness, authorities have not assessed its implementation.

9. **Development of the Cybersecurity Strategy – 2020-2025 and Strategic Plan.** SSSCIP considers the current Cybersecurity Strategy as effective between 2016-2020 as it was adopted in accordance with the National Security Strategy of Ukraine which ends in 2020. It would be timely to update the strategy and develop and approve a strategic plan for the same period, and into the future.
Ukrainian Cybersecurity Legal Framework: Overview and Analysis

Annex A

Legislative Framework on Cybersecurity in Ukraine

- Law No. 2163-VIII of 5 October 2017 on the Main Principles of Maintaining Cybersecurity of Ukraine;
- Law No. 2229-XII of 25 March 1992 on Security Service of Ukraine;
- Law No. 2135-XII of 18 February 1992 on Counterintelligence Activity;
- Law No. 3475-IV of 23 February 2006 on Ukraine State Service of Special Communication and Information Protection;
- Law No. 1280-IV of 18 November 2003 on Telecommunications;
- Law No. 3855-XII of 21 January 1994 on State Secrets;
- Law No. 2297-VI of 1 June 2010 on Personal Data Protection;
- Law No. 2469-VIII of 21 June 2018 on National Security of Ukraine;
- Law No. 851-IV of 22 May 2003 on Electronic Documents and Electronic Document Circulation;
- Law No. 3341-XII of 30 June 1993 on Organizational and Legal Framework on Fight against Organized Crime; and

Secondary Legislation on Cybersecurity in Ukraine

- President’s Decree No. 96 of 15 March 2016 on the decision of the National Security and Defense;
- Council of Ukraine dated January 27, 2016 “Cybersecurity Strategy of Ukraine”;
- President’s Decree No. 505/98 of 22 May 1998 on Regulating the Procedure for the Implementation of Cryptographic Information Security in Ukraine;
- President’s Decree No. 1229/99 of 27 September 1999 on Regulation on Technical Protection of Information in Ukraine;
- President’s Decree No. 184/2015 of 30 March 2015 on the decision of the Council of National Security and Defense of Ukraine dated March 12, 2015 “On the Status of Overcoming the Negative Consequences Caused by the Loss of Material Carriers of Classified Information in the Temporarily Occupied Territory of Ukraine in the Area of Anti-terrorist Operation in the Donetsk and Luhansk Oblasts” (classified, publicly not available);
- President’s Decree No. 32/2017 of 13 February 2017 “On the decision of the National Security and Defense Council of Ukraine” dated 29 December 2016 ‘On State Cyberthreats and Urgent Measures to Neutralize Them’;
- Cabinet of Ministers of Ukraine Resolution No. 1519 of 11 October 2002 “On Approval of the Procedure for Providing Confidential Communication Services to State Authorities and Local Self-Government Bodies, State Enterprises, Institutions and Organizations;
- Cabinet of Ministers of Ukraine Resolution No. 303 of 14 May 2015 “Some Questions of Organization of Interagency Information Exchange in the National System of Confidential Communication”;

29
• Cabinet of Ministers of Ukraine Order No. 1009 of 06 December 2017 “On Approval of the Concept of State System for CI protection”;

**List of Drafts Laws and Secondary Legislation**

**Daft Laws Registered in the Verkhovna Rada of Ukraine of 8th Convocation**

1) **Draft Law on Amending the Criminal Code and Code on Criminal Procedure to Delineate the Jurisdiction for Investigation of Crimes Committed in the Sphere of Use of Electronic Computing Machines (Computers), Systems, Computer Networks, Telecommunication Networks, State Information Resources and Critical Infrastructure Objects**, registered at the Verkhovna Rada as #8304, initiated by the Cabinet of Ministers of Ukraine. The draft was considered by the Committee on Legislative Support to Law Enforcement and was recommended for approval in the first reading by the Verkhovna Rada; it was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation;

2) **Draft Law on Amending Certain Legislative Acts of Ukraine to Strengthen Liability for Crimes Committed in the Sphere of Use of Electronic Computing Machines (Computers), Systems, Computer Networks, Telecommunication Networks, State Information Resources and Critical Infrastructure Objects, as well as Liability for Damaging Telecommunication Networks**, registered at the Verkhovna Rada as #8304-1 (as an alternative to #8304), initiated by MP Roman Semenukha (Samopomich). The draft was considered by the Committee on Legislative Support to Law Enforcement and was recommended for rejection by the Verkhovna Rada. The draft law was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation;

3) **Draft Law on Amending the Criminal Code of Ukraine (as Regards Strengthening Liability for Cyberterrorism and Cybercrime)**, registered at the Verkhovna Rada as #2328a, initiated by MP Ivan Myrnyi (Opposition Block). The draft had been under consideration by the Committee on Legislative Support to Law Enforcement since 2015; it was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation;

4) **Draft Law on Amending the Criminal Code of Ukraine (Establishing Liability for Cyberterrorism)**, registered at the Verkhovna Rada as #2439a, initiated by a group of MPs (Volodymyr Ariev (Petro Poroshenko Bloc), Svitlana Zalishchuk (Petro Poroshenko Bloc), Viktor Vovk (Oleh Liashko’s Radical Party), Iryna Herashchenko (First Vice-Speaker of the Parliament, close to the Petro Poroshenko Bloc), Leonid Yemets (People’s Front), Boryslav Bereza (non-partisan). The draft had been under consideration by the Committee on Legislative Support to Law Enforcement since 2015; it was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation;

5) **Draft Law on Amending Certain Laws of Ukraine (as Regards Strengthening Liability for Offences Committed in the Sphere of Information Security and Combating Cybercrimes)**, registered at the Verkhovna Rada as #2133a, initiated by a group of MPs (Andriy Kozhemyakin (Batkivshchyna), Vladyslav Bukharev (Batkivshchyna), Ruslan Lukyanchuk (People’s Front), Viktor Korol (Petro Poroshenko Block), Mykola Palamarchuk (Petro Poroshenko Block). The draft was considered by the Committee on Legislative Support to Law Enforcement and was recommended for approval in the
first reading by the Verkhovna Rada; it was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation;

6) Draft Law on Amending Certain Laws of Ukraine (as Regards Strengthening Liability for Offences Committed in the Sphere of Information Security and Combating Cybercrimes), registered with the Verkhovna Rada as # 2133a-1 (as an alternative to #2133a), initiated by MP Ihor Mosiychuk (Oleh Liashko’s Radical Party). The draft had been under consideration by the Committee on Legislative Support to Law Enforcement since 2016; it was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation;

7) Draft Law on Amending Certain Legislative Acts of Ukraine to Counter Threats to National Security in the Information Sphere, registered at the Verkhovna Rada as #6688, initiated by the group of MPs (Ivan Vynnyk (Petro Poroshenko Bloc), Dmytro Tymchuk (People’s Front), Tetiana Chornovol (People’s Front). The draft was considered by the Committee on National Security and Defense and was recommended for approval in the first reading by the Verkhovna Rada; it was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation;

8) Draft Law on Critical Infrastructure and Its Protection, developed by the Ministry of Economic Development and Trade and published for public discussion in July 2018. The draft law was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation. The draft was registered at the Verkhovna Rada as # 10328 on 27 May 2019; it was withdrawn after the termination of the mandate of the Verkhovna Rada of the 8th convocation.

Daft Laws Registered in the Verkhovna Rada of Ukraine of 9th Convocation

1) Draft Law on Amending the Law of Ukraine “On Protection of Information in Information and Telecommunication Systems” (Regarding Conformation of Information System Conformity to Information Protection Requirements)”, registered at the Verkhovna Rada on 3 September 2019 as No. 2043, initiated by MPs Oleksandr Fedienko and Mykhailo Kriachko (Servant of the People).

Secondary Legislation Drafts

1) Draft Resolution of the Cabinet of Ministers of Ukraine “On Approval of the Requirements for the Independent Audit of the Information Security of Critical Infrastructure Objects and the Procedure for Conducting an Independent Audit of Information Security at Critical Infrastructure Facilities”, developed by SSSCIP, published on its website for public discussion; this is the 4th version of the draft;

2) Draft Resolution of the Cabinet of Ministers of Ukraine “On Approval of the Procedures for Forming a List of Critical Infrastructure Objects, Recording Critical Infrastructure Objects in the State Register of Critical Infrastructure Objects, Its Formation and Ensuring Its Functioning”, developed by SSSCIP, published on its website for public discussion; this is the 2nd version of the draft;

3) Draft Resolution of the Cabinet of Ministers of Ukraine “On Approval of General Cybersecurity Requirements for Critical Infrastructure Objects, Criteria and Procedure for Assigning Objects to Critical Infrastructure Objects”, developed by SSSCIP, published on its website for public discussion; this is the 2nd version of the draft”. 
## Annex B

### Delineation of Powers between Ukrainian Authorities Responsible for Cybersecurity

<table>
<thead>
<tr>
<th>Authority</th>
<th>Cybersecurity Strategy</th>
<th>Law on Cybersecurity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ministry of Defense, General Staff</td>
<td>- counters military aggression in cyberspace (cyberdefense); - cooperates in the military field with NATO to ensure security of cyberspace and common protection from cyberthreats; - cooperates with SSSCIP and SSU to protect the Ministry of Defense’s informational infrastructure.</td>
<td>- counters military aggression in cyberspace (cyberdefense); - cooperates in the military field with NATO to ensure security of cyberspace and common protection from cyberthreats; - implements measures of cyberdefense for critical information infrastructure in case of emergency or martial law.</td>
</tr>
<tr>
<td>SSSCIP</td>
<td>- develops and implements state policy on the protection of state information resources; - ensures cyberdefense of critical information infrastructure; - coordinates activities of other cybersecurity agencies on cyberdefense; - prevents, detects and responds to cyber incidents and cyberattacks; - informs on cyberthreats and appropriate counteractions; - ensures functioning of State Center of Cyber defense; - audits the security of critical information infrastructure objects.</td>
<td>- develops and implements state policy on the protection of state information resources; - ensures cyberdefense of critical information infrastructure; - coordinates activities of other cybersecurity agencies on cyberdefense; - prevents, detects and responds to cyber incidents and cyberattacks; - informs on cyberthreats and appropriate counteractions; - ensures introduction of informational security audit on CI objects, establishes requirements to auditors, identifies the procedure of their certification (re-certification); - ensures creation and functioning of the National Telecommunication Network, introduction of organizational and technical model of cyber protection; - coordinates, organizes and conducts audit of communication and technological protection of CI objects from vulnerabilities; - ensures functioning of the State Center of Cyberdefense and CERT-UA.</td>
</tr>
<tr>
<td>SSU</td>
<td>- prevents, detects, terminates and investigates crimes against peace and security of humanity committed in cyberspace; - carries out counterintelligence and operational search activities to combat cyberterrorism and cyberespionage; - carries out counterintelligence and operational search to prepare CI objects to react in case of cyberattacks and cyber incidents and checks readiness of CI object to the potential cyberattacks and cyber incidents; - counteracts cybercrimes (which may influence vital interests of Ukraine); - investigates cyber incidents and cyberattacks on state electronic informational resources, critical informational infrastructure; - reacts on cyber incidents to state security.</td>
<td>- prevents, detects, terminates and investigates crimes against peace and security of humanity committed in cyberspace; - carries out counterintelligence and operational search activities to combat cyberterrorism and cyberespionage; - carries out counterintelligence and operational search to prepare CI objects to react in case of cyberattacks and cyber incidents and secretly checks readiness of CI object to the potential cyberattacks and cyber incidents; - counteracts cybercrimes (which may influence vital interests of Ukraine); - investigates cyber incidents and cyberattacks on state electronic informational resources, critical informational infrastructure; - reacts on cyber incidents to state security.</td>
</tr>
</tbody>
</table>
National Police
- ensures protection of human rights and freedoms, and public and state interest against cybercrimes;
- prevents, detects, terminates and investigates cybercrimes;
- raises public awareness on cybersecurity.

Intelligence agencies
- carries out intelligence activities on cyberthreats to the national security of Ukraine, other events and circumstances related to the sphere of cybersecurity.

### Roles of Cybersecurity Agencies

<table>
<thead>
<tr>
<th>International Cooperation</th>
<th>Cyber incidents/cyber-attacks/cyber threats</th>
<th>Protection of CI objects</th>
<th>Cybercrimes</th>
<th>State policies/public awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual assistance (Procurator General’s Office (pre-trial stage), Ministry of Justice (trial stage), Ministry of Foreign Affairs (in the absence of treaty))</td>
<td>SSSCP (all cyber incidents/attacks, CERT-UA, informing on cyber threats)</td>
<td>SSU (counter-intelligence and operational search, checking preparedness for cyber incidents and cyberattacks)</td>
<td>SSU (crimes against peace and security of humanity, which may influence vital interest of Ukraine, cyberterrorism and cyber-espionage)</td>
<td>SSSCP (policy on the protection of state information resources)</td>
</tr>
<tr>
<td>24/7 point of contact (Ministry of Justice (on courts’ commissions), Procurator General’s Office (bodies of prejudicial inquiry), Ministry of Internal Affairs)</td>
<td>SSU (CI objects, state security, state electronic resources, critical informational infrastructure, Cybersecurity Situation Center)</td>
<td>SSSCP (cyber defense, audit of CI object, introduction of independent informational security audit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ministry of Defense (military cooperation with NATO)</td>
<td>Intelligence agencies (intelligence activities on cyber threats)</td>
<td>Ministry of Defense (in case of emergency or martial law)</td>
<td>National Police (prevention, detection, termination and investigation)</td>
<td>National Police (public awareness on cybersecurity)</td>
</tr>
</tbody>
</table>