Eur J Secur Res
DOI 10.1007/s41125-017-0020-x

ORIGINAL ARTICLE

The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments

Lev Streltsov[1]

Received: 10 August 2017 / Accepted: 25 September 2017

Abstract Perceiving cybersecurity as one of the priority areas of national security is common among both developed and transitional states in today's globalized and digitized world. This is particularly relevant for the relatively young Independent state of Ukraine, which has during the last years repetitively fallen victim to many instances of high-profile malicious activity in cyberspace, the so-called "cyberattacks". In response, starting in 2015, a number of policy reforms aimed at developing the system of cybersecurity have begun to be implemented. Based on Ukrainian normative acts, the author attempts to describe the perception of cybersecurity, its defining features, the key principles of its provision, the system of actors that are involved in it, and the directions of sectoral policies, as well as their concrete measures. Furthermore, the article notes down the achievements that have already been reached and underlines the key challenges that are still to be overcome. Finally, the case study of Ukraine allows reaching some generalizations with regard

Important update! Cybersecurity, as a relatively young yet crucial area of national security develops at a rapid pace. On October 5th 2017, ten days after this article was approved for publication, the Ukrainian Parliament, after much deliberation and several redraftings over the last years, finally approved the Draft Law on the Foundations of the Provision of Cybersecurity of Ukraine (19.06.2015 №2126a). As is noted in the article, this is an immense milestone of Ukrainian regulation of cybersecurity. In terms of the challenges that are overviewed in the article, the draft's adoption, to an extent, solves some problems regarding doctrinal inconsistencies. Furthermore, it shifts the legal framework of the provision of this area of national security from regulatory to legislative. That said, the policy directions and the actors involved in cybersecurity, the distribution of roles between them, as well as various other aspects of regulation remain essentially the same. Therefore, it is still safe to use the article as a reference for understanding the system of cybersecurity of Ukraine. Apart from that, as noted in particular in Part 7 of the article, a number of challenges and policy directions are not and can be not solved by a single law and require their respective specialized measures, leaving them relevant and quite pressing.

✉ Lev Streltsov
L.streltsov@mpicc.de; LevStreltsov@gmail.com

[1] Researcher at Max Planck Institute for Foreign and International Criminal Law, Freiburg i. Br., Germany

Published online: 13 November 2017

to the approach of a state to establishing the functioning of this area of national security.

Keywords Cybersecurity · Ukraine · Cyberattacks · Cyberspace · National security

1 Introduction

Less than two months after the spread of the WannaCry ransomware in May, Ukraine faced yet another cyberattack, perhaps the most serious one in its history. Referred to as "Petya", "Petya.A", "PetrWrap", "GoldenEye", "Diskcoder.C", etc., the virus had quickly spread among Ukrainian systems, temporarily putting out of commission those of state bodies, airports, banks, media companies, delivery services and even the radiation monitoring systems at the former Chernobyl nuclear power plant! Damage was also done to many organizations abroad, including US Merck, Russian Rosneft, British WPP, French Saint-Gobain, Australian Cadbury, etc. (e.g. Roth and Nakashima 2017; Dearden 2017; Dudley-Nicholson and Bickers 2017; Nekrasov and Polyakova 2017; article of Business Censor of 27.07.2017). The speed of the malware's spread, the multitude of organizations harmed, including various objects of key infrastructure, as well as the serious obstacles to restoring the corrupted data once again underline today's priority of cybersecurity within the areas of national security of a state.

Cyberthreats of such scale are relatively new phenomena, or rather, with the constant increase of the globalization and digitalization of our world; they attribute existing phenomena with new features, thus allowing them to have a damage potential of incomparable scale. Since at the time of the writing of this article, the true nature of the "Petya" malware is uncertain, various experts believe it to be not ransomware but a disguised wiper (e.g. Brandom 2017; Gorodnikov 2017); it is safer to refer to "WannaCry" as an example. That malware spread itself around systems, encrypted files and provided the user with "ransom" demands for their decryption. One might attempt to imagine an analogy in a world without information technologies. A group of offenders makes their way into an office of an organization, breaks into a safe, steals several folders of documents and leaves a letter with ransom demands on the director's table. This crime would definitely harm the organization; some of its consumers, maybe business partners, perhaps go as far as harming the industry sector. In our world, however, the act, carried out in a digital environment, causes global chaos and a widespread panic.

These and other recent examples allow pointing out some of the features of cyberthreats that make them a priority for developing threat management mechanisms. First, a variety of factors, including their relative easiness of execution, as well as the problems with identifying the perpetrators and bringing them to justice, lead to constant actualizations of cyberthreats. For the last several months, the author has been monitoring the technology segments of global news and the days when there was no "hack" of something somewhere were very rare exceptions. Another important feature is their potential chaotic spread. This feature can be clearly seen from the WannaCry example, when the malware was able to

hamper the operations of railway operators in Germany, the Ministry of Internal Affairs of Russia, health sector organizations in UK, Indonesia and South Korea, industry in France, telecom and utility in Spain, delivery in the US, educational facilities in China, etc. (e.g. Goldman 2017; GReAT 2017; articles of Zeit Online and of BBC of 13.05.2017), i.e., multiple targets of various sectors, harming various interests including those of health and life. Lastly, although this is not a new finding at all, however, one that should always be stressed. Cyberthreats have no regards for geographical or political borders—they are truly global. Therefore, all political powers, organizations, associations, businesses, as well as each one of us should unite in order to produce common efforts in negating these perils of our reliance on technology.

Naturally, it would not be sensible to dedicate a single article to finding a solution for the world to unite to solve this problem. Rather, coming back to the "Petya" malware spread that caused by far the most damage to Ukraine, this publication focuses on the Ukrainian example of the state's approach to cybersecurity as a sphere of national security. Based on Ukrainian normative acts, the article attempts to establish what is seen as cybersecurity, what are key principles and approaches to its provision, what actors are involved in it, what policy measure are to be adopted, what are the achievements and what are the key challenges of the young independent state in this area of regulation.

2 Understanding Cybersecurity

To get a clearer perspective on the object of the analysis, first it is necessary to attempt to clarify what the Ukrainian state sees as cybersecurity and what are its main features. Unfortunately, it is not an easy task, partially connected to the uncertainty in the prescribed correlation between information security and cybersecurity in Ukraine. Originally, the latter was seen as a part of the former, which, in turn, was an essential element of national security of the state. Lately, however, on the regulatory level, a certain distinction seems to occur.

2.1 Legislation

The principal provision of the Constitution of Ukraine (Law, 28.06.1996 № 254к/96-BP) in this area is art.17 that states, "The protection of the sovereignty and territorial integrity of Ukraine, provision of its economic and information security are the most important functions of the state, a matter of the whole Ukrainian nation".[1] There is no mention of cybersecurity per se; however judging by the

[1] Official English translations of Ukrainian normative acts are usually unavailable. Therefore, the quotations and the names of the acts were translated by the author. The acts in their original language can be found on the Official Web-Portal of the Parliament of Ukraine (http://www.rada.gov.ua) by the requisites that the author provided in brackets after each one of them. Also, note that for easier reference, said requisites refer to the original adoption of the act or to a major reedition, not to the most current amendments.

spheres of protection that are seen as most important, it is safe to assume that cybersecurity falls into the area of information security.

One could attempt to find some answers in the Law "On Information"(Law, 02.10.1992 № 2657-XII), which regulates relations connected to information, the main aspects of state policy in the area, the right to information, its guarantees, establishes types of information, etc. However, the law is silent on the definition of information security and its connection to cybersecurity.

A much more useful source of normative provision is the Law "On the Fundamentals of National Security of Ukraine" (Law, 19.06.2003 № 964-IV). Art.7 defines nine main areas of threats to national interests and national security of Ukraine. They are the spheres of external politics, state security, military and border security, internal politics, economy, social and humanitarian, science and technology, civil defense, information. The threats connected to the sphere of information security that are listed in the act are: limitations of the freedom of speech and access to public info; dissemination of the cults of violence, cruelty and pornography by media; manipulation of the public conscience (e.g., by spreading false, incomplete or biased info); disclosure of state secrets or other restricted info that is essential for the protection of national interests; "computer crime" and "computer terrorism".

If there can be certain doubts about the fourth point (disclosure of restricted info), it is obvious that the final one definitely falls into the area of cybersecurity, effectively making cybersecurity a part of information security.

2.2 Academics

The findings of national legal researchers suggest a similar relationship. G.V. Foros and K.S. Kondrasheva state that "cybersecurity is the security of information and infrastructure in the digital environment" and "information security allows the attainment of such goals as the confidentiality of information; integrity of information and processes connected to it; availability of information; monitoring of all such processes" (Форос, Кондрашева 2016, p.101–102). First, one can notice the similarity between the definition of information security and the respective category of crimes of the Council of Europe Convention on Cybercrime.[2] However, even without highlighting this resemblance, the definitions of information security and cybersecurity provided by the academic definitely indicate that two concepts are intertwined.

This can be also inferred from the opinion of O.V. Kosarevska and O.I. Novitsky (Косаревська, Новіцький 2016, p.104–106) who speak of threats to information security that manifest themselves through negative informational influence on the conscience and behavior of citizens and through such influence on informational resources and informational and technical infrastructure. They follow up with such statements as "guaranteeing effective counteraction to cybercrime can be achieved only by enforcement of complex approaches to the establishment of information security" and "counteraction of cybercrime should be an element of state policy of information security".

[2] Ch.II Sect. 1 Title 1Offences against the confidentiality, integrity and availability of data.

2.3 Regulations

According to the above stated, it is possible to assume that the hierarchy here is: information security—cybersecurity—cybercrime counteraction. The regulatory level, however, makes things far less simple. Turning to the Strategy of National Security of Ukraine,[3] one can notice that art.3 speaks of threats to information security (para.6) and threats to cybersecurity and security of informational resources (para.7). The first category comprises the conduct of informational warfare against Ukraine and lack of a coherent communication policy of the state, an insufficient level of media culture of the society. An oversimplification, but this area of threats can be seen as one connected mainly to external ideological influence. On the other hand, threats to cybersecurity and security of informational resources include the vulnerability of objects of key infrastructure and state information resources to cyberattacks; physically and morally obsolete system of protection of state secrets and other restricted information. A similar differentiation can be noted in provisions of the Concept of Development of the Security and Defense Sector of Ukraine.[4]

The Doctrine of Informational Security of Ukraine[5] that is aimed at the establishment of directions and priorities of national policy in the area of information also has the above-mentioned "ideological" angle. However, some provisions seem to lie in the area of cybersecurity, an example can be art.5.1 that speaks of the restriction of information transmission through computer networks in a state of martial law. Still, as a general rule, para. 3 of art.1 states that the principles, priorities and directions of establishment of cybersecurity are provided by a separate normative act—the Strategy of Cybersecurity of Ukraine.[6] This strategy regulates several areas of cybersecurity, including the protection of state information resources, key infrastructure, counteracting cybercrime, etc. Its provisions are presented in more detail in the following parts of the article. At the same time, the penultimate paragraph of art.1 of the Doctrine of Informational Security mentions that the development and security of cyberspace, establishment of electronic governance, security and sustainable functioning of electronic communication and state electronic informational resources are to be elements of the state policy in the area of development of informational space and development of the informational society in Ukraine. This adds up to the confusion.

2.4 What is the Correlation?

Although it is not easy to sum this part up with a definite conclusion, the following may be assumed. Currently, at least on the level of regulatory acts, information security and cybersecurity are two spheres of national security that possess different defining qualities. For information security, this is the object of impact (personal or mass conscience, etc.) of the threat. For cybersecurity—not so much the object, as

[3] Enacted by Presidential Decree of May 26, 2015, № 287/2015.

[4] Enacted by Presidential Decree of April 14, 2016, № 92/2016.

[5] Enacted by Presidential Decree of February 25, 2017, № 47/2017.

[6] Enacted by Presidential Decree of March 15, 2016, № 96/2016.

the dimension (digital environment, cyberspace, etc.). Thus, a "cyberterrorist" that remotely hacks an automated management system of a power plant does not (directly) harm informational security, neither does disseminating false-printed propaganda harm cybersecurity. At the same time, hacking a governmental website and altering the information that is presented there negatively impacts both spheres. Such a correlation does not allow the spheres to be either subordinate or alternative.

This paper, however, is not aimed at establishing a strict definition. Rather, it aims to point out the flaw in the establishment of the borders of the spheres of national security in Ukraine, which exists on both the normative and academic levels. Furthermore, it is imperative to underline that cybersecurity is not defined at all on the legislative level. Hopefully, this will be partially resolved with the probable adoption of the Draft Law on the Foundations of the Provision of Cybersecurity of Ukraine (Draft law, 19.06.2015 №2126a), which is analyzed further. Thus, a necessity of in-depth research of this question with a further goal of drafting and adopting a consistent legislative framework is strongly advocated.

Still, for the purposes of this publication, it is possible to operate with the somewhat broad definition that is presented in para.10 art.1 of the Strategy of Cybersecurity:

> "… condition of protection of vital interests of persons and citizens, society and state in cyberspace that is achieved by a complex utilization of a totality of legal, organizational, informational measures…"

2.5 The Main Features of Cybersecurity

Although terminological aspects remain unresolved, an analysis of provisions of the above-mentioned acts allows pointing out several key features of the understanding of cybersecurity and its features by the Ukrainian state.

The first feature, although a bit obvious, still needs to be stated. The regime understands the importance of protection of interests connected to cyberspace. This can be inferred from para.1 of art.1 of the Cybersecurity Strategy, where the multilevel benefits of an "open and free cyberspace" are listed, the part of the aforementioned cybersecurity definition (para.10 art.1) that describes cybersecurity as "… protection of vital interests of … in cyberspace", the combination of provisions of para. 5, 6 and 9 of the article that speaks of creation of the conditions for a safe cyberspace by providing "cybersecurity of state electronic information resources, information that requires protection by law, information infrastructure…" etc. In addition, after all, as mentioned above, cybersecurity is defined as one of the key areas of national security by art.3 of the Strategy of National Security of Ukraine.

The second feature is connected to understanding cybersecurity as a threat-based, risk-management function. This can be inferred from the aspect of the noted definition of cybersecurity being "a condition of protection". Apart from that, acts of a more general level that regulate national security in general (the provisions of which should apply to all its spheres) provide further indications of this nature of the state function. For instance, para.1-2 of the Strategy of National Security establishes

the minimization of threats to state sovereignty as one of its main goals and the Law on National Security, in art.1 defines national security as "protection of vital interests …, prevention and neutralization of real and potential threats". Moreover, the structure of acts connected to areas of national security allows seeing that the provided regulations are threat-based, with a "threats" section being presented right after the introductory provisions or the "protected interests" section.

Finally, the third feature lies in the adoption of a systemic approach to cybersecurity provision. Thus, it is understood that establishing a functioning framework of cybersecurity requires a coordination of different sectoral policies and employment of capabilities of various actors, both state and private. This feature is seen first of all from the part of the cybersecurity definition that speaks of "… cybersecurity … achieved by a complex utilization of a combination of legal, organizational, informational measures" and furthermore by the provisions of art.3 and art.4 of the Strategy that, respectively, regulate the parties involved in cybersecurity and perspective directions of its development. These particular aspects receive their attention further in the paper.

3 Threats to Cybersecurity

Having established the threat-based nature of cybersecurity, it is possible to proceed with overviewing the actualized threats thereto, those, which the state of Ukraine has been facing over the last years.

3.1 The Threats

"Petya" malware The first wave of infection took place on June 27 2017, affecting systems in various organizations: state bodies, airports, banks, media companies, delivery services and even the radiation monitoring systems at the former Chernobyl nuclear power plant. The largest number of infections was carried out through a scheme where the malware would gain access to computers through trusted software, in this case, an accounting application (as mentioned in an article in Tech Today of 04.07.2017). According to the information of the Cyberpolice, the software (M.E.Doc) was corrupted by means of illegal access to one of the computers of its developer-company (stated on the Cyberpolice official website on 05.07.2017). Parallel to that, the infection was spread by more "conventional" means: through e-mail attachments (further mentioned in the Tech Today article of 04.07.2017). In both cases, once the malware had gained access to target systems, it proceeded to encrypt files, reboot the system and start it again with a ransom message, asking to send funds to a bitcoin wallet. At the same time, various experts believe that ransom was not the perpetrators aim here, the malware's prime function was to corrupt data and it had only been masked as ransomware (e.g. Gorodnikov 2017; Brandom 2017).

Energy sector December 25, 2015 was the date of one of the first registered successful cyberattacks on energy systems in the world. Perpetrators managed to successfully attack computer management systems of three energy companies of

Ukraine. The main harm was done to "Prikarpattyaoblenergo": 30 substations were shut down; around 230 thousands (!) of people were left without electricity for up to 6 h.

The attack was carried out as a complex of actions: first, networks were infected by a trojan (Black energy) that was delivered via forged emails. That was followed by taking control of automated remote control systems and executing shutdown operations on substations. To create obstacles for getting the substations operational again, the perpetrators continued to remotely disable elements of IT infrastructure (uninterruptible power supplies; modems; remote technical units; network switches), deleted information on servers and workstations (with a killdisk utility). Finally, in order to create additional chaos and confusion, DDoS attacks were carried out against call centers of energy providers, which did not allow them to function properly.[7]

It is worth to note that a similar by nature attack (but of lesser scale) was carried out in December 2016 against the "Pivnichna" substation, leaving a part of the capital without power for an hour and a quarter.

2014 Presidential Elections The attack was carried out against the automated election system "Vibori" during the Early Presidential Elections in May 2014. The system that was supposed to show the intermediary results of the elections in real time was compromised. Following that, on May 25, minutes before the end of the elections, the perpetrators uploaded a fabricated image on the servers of the Central Elective Committee that depicted the elections being led by a candidate who was known for his rather nationalistic views. Furthermore, this image was used by central Russian media to illustrate the election process in Ukraine, supposedly leaning to support of such views. Lastly, the next day, the servers that were tasked with receiving and processing data connected to counting the votes were subjected to a DoS-attack, rendering them inaccessible for about 2 h. This attack can be seen as multifaceted, a system of acts that were aimed at achieving different objectives. It also serves as an illustration of a cyberattack that threatens not only cybersecurity but also information security, as these spheres are defined in the regulatory acts of last years (discussed earlier).

According to N. Koval (Koval 2015, p.56–57), these actions were probably the most technically advanced cyberattack that had by that time been investigated by CERT-UA.[8] Although sole responsibility was taken by the CyberBerkut organization, the specialist believes that the attack was too complex to have been carried out without support of a stronger power.

Cyberattacks of 2016 Several attacks have been carried out during the previous year. Due to a number of factors, not so much information about them is in the public domain. Amongst such acts are the December 6 attack on state financial

[7] According to the statements of Ukrainian officials, access to the networks was gained via the Internet, through the subnetworks that belong to providers in the Russian Federation. See e.g. http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109.

[8] Computer Emergency Response Team of Ukraine, a specialized division of the State Service of Special Communications and Information Protection.

organizations, including the State Treasury of Ukraine and the State Pension Fund, leading to substantial delays in budget payments, which was carried out with the utilization of similar software as was used in the energy sector attack (Nekrasov 2016). Other cybersecurity threats of 2016 were connected to the hackings of Regional State Administrations[9] and the identification of malware in the electronic flight control system of the Borispil national airport (Парфило, Нізовцев 2016, p.79).

"Euromaidan" events The events that manifested in the end of 2013—beginning of 2014 were followed by various kinds of malicious cyberactivity. It included blocking of mobile communications by means of mass automated calls to devices of key political actors, hacks that lead to several electronic media websites going offline (Дубов 2014, p.214), or utilization of netbots to spread false information or "informational waste" in social networks. Amongst others were hacks of personal e-mails and social network accounts of politics, DDoS attacks aimed at state bodies, including the Ministry of Internal Affairs, the Cabinet of Ministers, the President and the General Prosecution Office of Ukraine. Furthermore, an infection of information systems of state bodies (including law-enforcement), media, financial entities, large industry companies was carried out with a utilization of a worm (with a rootkit) called by different sources as "snake", "ouraboros" or "turla". The main goals of the perpetrators were theft of confidential information and/or protracted monitoring of said information.[10]

A point worth noting here is that the acts surely lie in both the areas of cybersecurity and information security, further suggesting the necessity to establish a proper relationship between the two areas on both theoretical and legislative levels.

EX.UA "Hacktivism" An event of 2012 that could have been seen as a "taste of things to come". Ex.ua was a file-sharing service that allowed mass-scale illegal distribution of copyright-protected material (audio, video, computer programs, video games, etc.)

Ukrainian law-enforcement bodies blocked the domain and physically seized the company's servers. The problem was that the service had been actively used by a large amount of the population. Therefore, the same day successful DDoS attacks had been launched against a dozen of governmental websites, including the website of the President, the Parliament, the State Security Service and the Ministry of Internal Affairs, blocking their functioning. The specificity of this attack is that it was carried out mainly by "generic" citizens, coordinated by social networks, with the utilization of easy to use services, such as the "Low Orbit Ion Cannon".

[9] There is not too much information in the public domain, however according to an official press release of the Security Service of Ukraine, at the time of said release, its operatives had detected a number of said hacks and initiated 25 criminal proceedings. https://ssu.gov.ua/ua/news/1/category/21/view/1228#sthash.eKeO6uu0.dpbs.

[10] See materials of the CERT-UA website:
http://cert.gov.ua/?p=714
http://cert.gov.ua/?p=506
http://cert.gov.ua/?p=344.

This was the first major instance of a hacktivist cyberattack in Ukraine, but as noted by D.Dubov (Дубов 2014, p.214), since no direct financial harm was done to state bodies, no criminal cases were instigated and, what is more unfortunate, no real conclusions about the state of Ukrainian cybersecurity were made.

Generic cybercrime All the events referred to above were in national or even international news' spotlights. However, on a day-to-day basis, numerous criminal activities, commonly referred to as cybercrimes, are also taking place. Amongst them are instances of cyber fraud, content-related offences as well as using and/or selling software designed to gain illegal access to computers and networks. A more detailed overview as well as several examples are provided further in the article.

Non-intentional malfunctions When speaking of cybersecurity, one needs to keep in mind another potential type of threats. Not all malfunctions in automated systems can be intentional—some can be attributed to unintentional forms of guilt, others can come out of pure force majeure. There is not so much available data on actualizations of such threats in Ukraine; however, a well-known relatively recent example occurred on the weekend of May 27–28, 2017 in UK Heathrow and Gatwick Airports when a mass "computer crash" affected British Airways booking systems, baggage handling, mobile phone booking apps, check-in desks, etc. effectively disrupting travel for several days (as noted, for example, in an article of The Guardian of 28.05.2017). Another, even more recent incident is the malfunction of the autopilot of cargo ship ACX Crystal that leads to a deadly collision with US destroyer USS Fitzgerald on June 23, 2017 (Gertz 2017).

3.2 Classifications

From the given examples, it is possible to see that threats can be of different nature, the results of actions of different actors that have different motives. They can be aimed at many objects, possess various magnitudes, create different victims and as a result—a multitude of harmful consequences. An approach where all the above incidents are regarded as cybercrimes may be doctrinally correct (apart from the malfunctions that entail no form of guilt); however, it does not provide much from the practical point. Law-enforcement capabilities might prove insufficient to deal with a foreign intelligence service cyberattack on a key infrastructure object—that is where specialized counterintelligence or military actors need to be employed. On the other hand, these evidently should not be utilized to negate, for example, consequences of a hack into a social network account of a celebrity with the intent to acquire compromising pictures. In this case, regular law-enforcement seems more than sufficient. Furthermore, returning to purely unintentional incidents, neither of the above-mentioned organizations should take lead in their management: this is a question for technical protection authorities or even for the private sector.

The key point of these deliberations is that the qualities of each threat should be assessed, and a combination of measures and capabilities of various structures should be utilized as a proportionate management mechanism. This understanding is fully consistent with the systemic approach to provision of cybersecurity and further

underlines its importance. At the same time, a creation of "templates" of response mechanisms, tailored to types of threats, first of all, requires the creation of a proper typology of threats, their classification.

Unfortunately, Ukraine is still far from its creation. For example, the CNSD[11] Decision "On the Threats to Cybersecurity of the State and Imminent Measures of their Neutralization"[12] is surprisingly silent on actually listing said threats, limiting itself to provisions of the preamble that underline the current "crisis condition" of cybersecurity, which is a "threat to national security". That said, the document is quite useful since it does provide for a list of measures that are to be carried out in specified timeframes of the nearest future. They are overviewed in detail in the following parts of the article.

As was mentioned earlier, the Strategy of National Security lists two main threats to cybersecurity, which are the vulnerability of objects of key infrastructure and state information resources to cyberattacks; physically and morally obsolete system of protection of state secrets and other restricted information (art.3.7). At the same time, it is possible to argue that these are not threats, rather some of the factors that allow for actualizations of threats.

Continuing the analysis, it is possible to refer to the first four paragraphs of art.2 of the Strategy of Cybersecurity; however, the presented system is somewhat inconsistent, the concepts are undefined and seem overlapping. The provisions speak of cyberwarfare; intelligence and subversive activity of foreign special agencies; cyberattacks that can be aimed at informational resources of financial institutions, transport and energy, public authorities that are engaged in the provision of security, defense and protection from emergencies. Furthermore, if such attacks lead to the violation of the modes of operation of automatized processes in the objects of key infrastructure, they can amount to cyberterrorism. Another mentioned type of widespread cyberattacks is politically motivated acts against governmental or private websites that alter the provided information or effectively block access to it.

Finally, the Strategy notes that the current state of development of the information society allows for both new means to carry out traditional crimes and for the emergence of new crimes, therefore adding "generic" cybercrime to the list of threats to cybersecurity. In this sense, it speaks of the increase of instances of illegal collection, storage, use, deletion of personal data, illegal financial operations, theft and fraud over the Internet (art.1 para.3).

The categorization attempt of D. Dubov presents a more consistent approach to the cyberthreats to the Ukrainian state and society: "classical" cybercrime (fraud, extortion, illegal access to personal information and automated databases, spread of pornography, weapons and narcotics sales, etc.) and cybercrimes that are characteristic to geopolitical conflict (hacktivism, cyberespionage and cyber-sabotage). At the same time, the researcher notes that it is hard to separate the crimes because of the application of same methods, for example, phishing

[11] Council of National Security and Defense.

[12] Enacted by Presidential Decree of February 2017 №32/2017.

techniques can be used for theft of funds of persons as well as for cyberespionage (Дубов 2014, p.210). Furthermore, he omits the category of unintentional incidents.

In an attempt to look for inspiration, one may to address the Cybersecurity Strategy of the European Union.[13] Art.1.1 once again underlines the fact that threats can have different origins—"including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes". An important phrase used in the same article is "cybersecurity incidents, be it intentional or accidental". Defining an actualized cyberthreat, regardless of its origin, as a "cybersecurity incident" is a valid starting point. This concept is also used in the Ukrainian Draft Law that was mentioned earlier and on which more focus is placed later in the article.

As to an actual classification, the EU Strategy is also lacking a complete one, although some approaches can be inferred from its provisions. For instance, art. 3.1 speaks of institutional structures "to deal with cyber resilience, cybercrime and defense". Therefore, it is possible to see such categories of cyberthreats as threats to cyber resilience, cybercrimes and threats to cyberdefense. Furthermore, the provisions of art.3.2 that define the roles of different actors in response to different types of incidents, mention such features of incidents as: "has a serious impact on the business continuity", "seems to relate to a crime", "seems to relate to cyber espionage or a state-sponsored attack, or has national security implications", "seems having compromised personal data", etc.

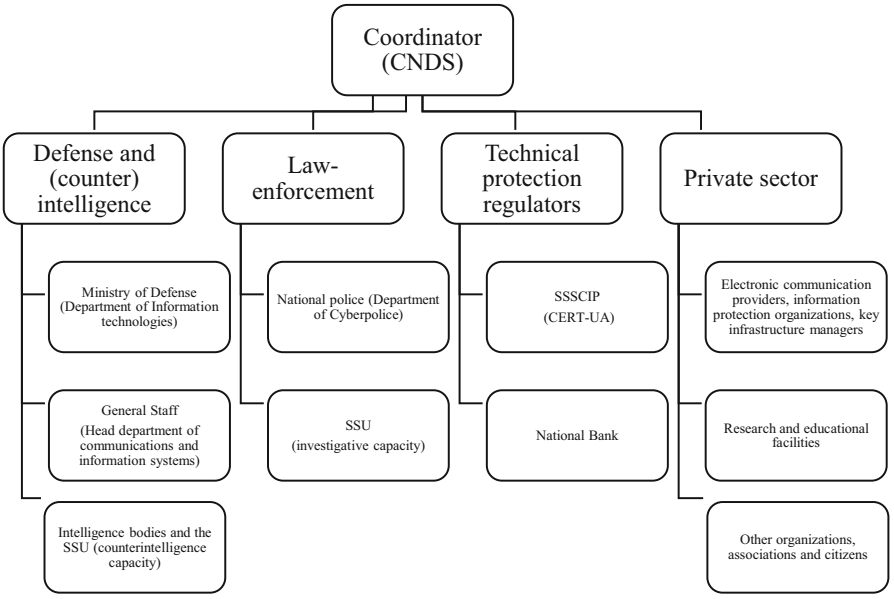
Although a single, exclusive classificatory criterion is not established, it is possible to utilize the Strategy's approaches to attempt to classify threats to the cybersecurity of Ukraine. The threats may be divided into three broad categories: threats aimed at cyber defense—actions directed at key infrastructure or informational resources (regardless of the actor, be it a hostile state, a "hacktivist" organization, a terrorist group, etc.); "generic" cybercrimes (aimed mainly at interests of private entities and not the society in general) and threats to cyber resilience (non-intentional cyberincidents). Once again, it is necessary to restate that the cybersecurity system of Ukraine should be established with a view to counteract all of these threats, with a combination of measures and delegation of authority to respective structures.

4 The System of Actors

Having provided an overview of threats to Ukrainian cybersecurity and reflected on the question of their classification, it is possible to move on to establishing the main actors in this area of national security and their roles in its provision. Unfortunately, today the legal basis of the system of said actors as a whole is provided mainly by art.3 of the Cybersecurity Strategy, which is a document of the regulatory level and furthermore drafted in rather general terms, without in-depth specification of tasks

[13] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013. JOIN(2013) 1 final.

or establishment of interaction mechanisms between actors. Nevertheless, an analysis of its provisions allows constructing the following chart, based on four pillars with a coordinating body.



The Coordinator The Council of National Security and Defense carries out the coordination and control of the activity of the subjects of the Sector of Security and Defense[14] that enforce the cybersecurity of Ukraine. The area-specific body of the Council is the National Coordination Center of Cybersecurity. Amongst its tasks[15] are analysis of the state of cybersecurity and various parameters thereof; prognostication and detection of cyberthreats; development, implementation and supervision of cybersecurity measures' propositions (including measures of information exchange between actors and measures of international cooperation), etc.

An example of the functions of the Center could be seen in its response to the Petya incident: the Center provided security recommendations to state establishments including their connection to a protected perimeter. It has been reported that none of these establishments were damaged. Furthermore, the Center had taken lead on enforcing a rapid response protocol together with other actors that allowed stopping further spread of the malware.[16]

[14] In principle, the Sector of Security and Defense of Ukraine encompasses military, intelligence, state security and law-enforcement bodies. At the same time, the decisions of the Council and the measures taken by the bodies that it coordinates can have impact on all other actors involved in cybersecurity provision, effectively making the Council the general coordinator.

[15] Prescribed by Provision on the National Coordination Center of Cybersecurity, enacted by Presidential Decree of June 7 2016, № 242/2016.

[16] See official website of the CNSD: http://www.rnbo.gov.ua/news/2817.html.

Defense and (counter) Intelligence Structures The military structures of this pillar are represented by the Ministry of Defense and the General Staff of the Armed Forces. Their main tasks in the area of provision of cybersecurity are repelling military aggression in cyberspace; military cooperation with NATO in the areas of cybersecurity and mutual protection from cyberthreats; cyberprotection of informational infrastructure of the armed forces.[17] The specialized divisions of these structures are the Division of Information Technologies of the Ministry of Defense and the Head Division of Communications and Information Systems of the General Staff. Furthermore, the Minister of Defense of Ukraine has recently announced the development of a new unit, with consideration of the positive experience of Lithuania and with assistance from NATO.[18]

The intelligence bodies, which include the Service of External Intelligence of Ukraine, the Intelligence Body of the Ministry of Defense of Ukraine, and the Intelligence Body of the State Border Guard, have their general legal base of functioning provided by the Law on Intelligence Bodies of Ukraine (Law, 22.03.2001 № 2331-III). In the area of cybersecurity, they are tasked with carrying out intelligence activity concerning threats to national security in cyberspace, or other events and circumstances in the area of cybersecurity.

The Security Service of Ukraine is in a somewhat special position in the system, since it acts in a twofold capacity as a counterintelligence and specialized law-enforcement body. In its first capacity, its main cybersecurity tasks are: counter-intelligence and investigative measures aimed at fighting with cyberterrorism and cyberespionage, evaluation of the preparedness of key infrastructure objects to possible cyber incidents; reaction to cyber incidents in the area of national security, etc.

Law-Enforcement Bodies One key actor of this group is the Security Service of Ukraine, acting in its law-enforcement capacity. In this capacity, its functions in the area of cybersecurity are investigation of incidents connected to state information resources and other information that requires protection, of key informational infrastructure. The Service furthermore is tasked with prevention, identification, stopping and solving cybercrimes against the peace and security of humanity, or those, the consequence of which directly creates a threat to vital interests of Ukraine.

The other key actor is the National Police of Ukraine. In the area of cybersecurity, its functions are: enforcement of the protection of rights and liberties of persons and citizens, interests of the society and the state from criminal violations in cyberspace; prevention, detection, stopping the commission of and solving cybercrimes; increasing the cybersecurity awareness of citizens.

Focus on the specialized units of these bodies, as well as more details of the execution of their functions, is provided in the next section of the article.

Technical Protection Regulators This group is mainly represented by the State Service of Special Communication and Information Protection. Its tasks are forming

[17] Jointly with the State Service of Special Communication and Information Protection and the Security Service of Ukraine.

[18] https://www.ukrinform.ru/rubric-community/2256867-v-ukraine-sozdaut-kibervojska-poltorak.html.

and implementing state policy, state control of cyberprotection of state information resources and other information that requires protection, of key informational infrastructure. Apart from that, it carries out organizational and technical measures of prevention, identification and reaction to cyberincidents, elimination of their consequences, providing information on cyberthreats and respective methods of protection; auditing the objects of key informational infrastructure for vulnerabilities, etc. The structure of the Service includes a specialized division, CERT-UA (Computer Emergency Response Team of Ukraine), which is directly responsible for counteracting the most serious cyberthreats to the state with technical means.

Another important actor of the group is the National Bank of Ukraine that is tasked with the establishment of requirements towards cyberprotection of critical information infrastructure in the banking sphere.

The Private Sector Although the Strategy does not directly give instruction to private sector actors, it does speak of the necessity to create the conditions for their participation in the following capacities. The first type of actor here is organizations that carry out activity in the area of electronic communications, information protection and/or are owners (managers) of key infrastructure objects. These organizations are to take part in the provision of cybersecurity of Ukraine, namely through obliging them to implement protection measures and to cooperate with state bodies in their respective tasks in the given area. Another form of participation of non-state bodies is the involvement of scientific and research organizations, educational facilities (as well as other organizations, public associations and citizens) in development and implementation of cybersecurity measures.

Unfortunately, the area of public–private partnership is only at an early stage of its development. As noted by D. Dubov, particularly with regard to the research and scientific aspects of it, Ukraine is severely lacking efficient specialized research institutions of the cybersecurity area (Дубов 2014, p.255). Furthermore, if we speak of the aspects of cooperation between state bodies and business oriented organizations, the legal framework of such cooperation is also something that requires much work before it can properly function. At the same time, it is worth to note that these problems are not intrinsic only to Ukraine—questions of the functioning of public–private partnership are debated even in states with the most developed legal systems.

5 The Role of Law Enforcement

The previous section of the publication has partially illustrated the limitation of the role of law-enforcement bodies in the provision of cybersecurity of the state; law-enforcement can be seen as but one of four pillars on which the system stands. At the same time, as limited as it can be, it fills its key niche and must function to its full potential.

5.1 The Actors

It has been noted that the Security Service of Ukraine has a twofold capacity: counterintelligence and investigative. Its main legal base of functioning is the Law "On the Security Service of Ukraine" (Law, 25.03.1992 № 2229-XII). Its main counterintelligence department in the area of cybersecurity is the Unit of Counterintelligence Protection of the Interests of the State in the Sphere of Information Security. Here, however, focus should be placed on its latter capacity—investigative activity with regard to cybercrime. Depending on the type of crime, this task can fall under the authority of different units of the Service. It is worth to note that when acting as an investigating body, the Service is bound by the general provisions of the Code of Criminal Procedure (Law, 13.04.2012 № 4651-VI) and not by specialized (counter) intelligence procedures. According to official statements, in the area of cybersecurity, its law-enforcement functions include "fighting cyberterrorism; fighting cybercrime that endangers vital interests of the state; control of the circulation of special technical measures of covert information acquisition" (Дубов 2014, p.214), etc.

The more general law-enforcement actor is naturally the National Police, which deals with the majority of cybercrimes. Its main legal base of functioning is the respective provisions of the Code of Criminal Procedure and the Law "On National Police" (Law, 02.07.2015 № 580-VIII). It is necessary to note that the police has been going through a series of structural reforms, including the re-attestation of its staff; even more reforms are planned in the nearest future. The current specialized division operating in the area of cybercrime counteraction is the Department of Cyberpolice[19] that functions in particular according to the Provision on the Department of Cyberpolice.[20]

Its two chief tasks[21] are taking part in the prevention and counteraction of criminal offences connected to the use of electronic-computational devices, systems, computer networks and telecommunication networks; provision of assistance to other units of the National Police in preventing, detecting and stopping the commission of criminal offences carried out with the utilization of said objects.

The functions of the Department are further clarified in part III of the Provision, which lists 23 of them, including a cover-all "other functions according to legislation" provision. The most obvious ones are the direct function connected to solving crimes—carrying out investigative actions in criminal proceedings, as well as establishing and maintaining a 24/7 contact network connected to crime reporting, prosecution of the accused and collection of electronic evidence. At the same time, the Department is to carry out diverse analytic functions with regard to factors that lead to the commission of cybercrimes, information on criminogenic processes and the state of crime counteraction, as well as data on individual cyber

[19] Established by the Resolution of the Cabinet of Ministers of Ukraine №831 of October 13, 2015 № 831.

[20] Enacted by the Order of the National Police of Ukraine of November 10, 2015 № 85.

[21] Part II of the Provision.

offences. Furthermore, the Department plays its part in developing legislative measures by introducing proposals on improvements of legislation and other normative acts in the area of cybercrime counteraction (including by means of studying national and foreign experience). Finally, the Department carries out educational activity: drafts professional development guidelines for bodies of the National Police; carries out community outreach and educates the public on questions of cybersecurity in day-to-day life; takes part in trainings, conferences, seminars, etc.

Two points are to be made here. The systemic approach to cybersecurity provision can be seen even within the diversity of activities of one of the actors of one of its pillars. The Cyberpolice is tasked with carrying out crime-solving, analytic, measures-drafting, educational and other functions. The second point is connected to the fact that although the "tasks" of the Department include crime prevention, the "functions" do not indicate direct ways of carrying out such activity, it seems to manifest only indirectly, through the fulfillment of others. This once again raises the debatable question of the nature of crime-preventive functions of law-enforcement bodies.

For example, as pointed out by I.P. Katerinchuk, cybercrime counteraction consists: of crime prevention, organization of said counteraction and enforcing criminal responsibility (Катеринчук 2016, p.6), i.e., bringing the guilty to justice. In this regard, it can be seen that only the third function completely lies in the field of law-enforcement powers, since the researcher further clarifies that: organization relates more to administrative law. In turn, prevention, according to the academic, consists of various measures, amongst which are economic, ideological, legal, educational, technical, cryptographic, etc. (Катеринчук 2016, p.6) Thus, the impact that the actual enforcement of the law has on crime prevention seems to be limited in this area of illegal activity, perhaps even more than in others.

At the same time, a number of researchers point out new trends in criminal legislation that allow increasing the scope of the preventive functions of criminal law.[22] One may assume that if the legislation follows such trends, bodies that enforce it will also, to an extent, exercise a more preventive approach in regards to criminal activity. However, the degree of this in relation to Ukraine and its system deserves a separate in-depth analysis.

5.2 The Crimes

There are various ways to classify cybercrimes. One of the most widely accepted is the classification of the Council of Europe Convention on Cybercrime.

Offences against the confidentiality, integrity and availability of computer data and systems Responsibility for this category is mainly prescribed by a separate Chapter XVI of the Special Part of the Criminal Code of Ukraine (Law, 05.04.2001 № 2341-III) "Crimes in the area of the use of electronic-computational machines (computers), systems, computer networks and telecommunication networks". This

[22] See further Sieber/Vogel 2016 e.g. pp. 137–145, 211–214 (mostly on terrorism-related offences) or Carvalho 2017 for a more general approach.

Chapter was introduced into the Criminal Code 2001 edition and its contents went through a series of changes, the most notable of which occurred in 2003, 2004 and 2014.

Today it consists of the following crimes: art.361—unsanctioned interference in the operation of computers, networks; art.361[1]—creation or distribution of malicious programs or technical devices designed to carry out such interference; art.363[1]—interference with the work of computers by means of mass distribution of telecom messages;[23] art.361[2]—unsanctioned distribution of information with restricted access stored on computers; art.362 p.1—unsanctioned actions with information stored on computers by persons with a right of access; p.2 unsanctioned interception or copying of information by said persons; art. 363—violating the order of usage of computers that leads to substantial harm by persons responsible for their usage.

All these crimes can be carried out under specific aggravated circumstances, which usually include being committed by a group of persons, or resulting in severe harm (currently 80000 UAH, approx. 2550 EUR). The possible penalties vary between fines, imprisonment for up to 5 years and prohibitions to carry out certain activity or to occupy certain positions.

> A high-profile example of this type of crime is naturally the Petya malware infection. According to a statement of the Head of the Department of the Cyberpolice, by July 5th 2017, 597 (!) criminal proceeding were initiated, preliminary qualifying the offense as a crime prescribed by art. 361 (According to an interview of the Head of Cyberpolice of Ukraine of 05.07.2017). [24]

> In contrast, a relatively recent example of a low-profile case (verdict of 21.03.2017) is № 640/953/17, where a group of persons was found guilty in the online sale of software designed to carry out DDoS attacks «Overflow Bot» (art.361[1]). Furthermore, in order to demonstrate the operability of said software, the perpetrators carried out several DDoS attacks (art.361).[25]

Apart from the listed offences, the Criminal Code establishes responsibility for other offences, those connected to accumulation and disclosure of specific types of restricted info. Today many of such crimes can be carried out through the use of computers and/or networks. Among them are espionage (art.114), certain types of treason (art.111), gathering or transmitting information gathered in the course of investigative, counterintelligence activity, in the sphere of state defense (art.330), military information (art.422), illegal gathering or utilization of commercial or

[23] Do note that this article does not criminalize DoS or DDoS attacks, the "mass distribution" refers to sending messages to a multitude of non-specific recipients and not from a multitude of computers to a single one. Thus, this crime usually refers to spam with a malware component.

[24] Цензор.нет (05.07.2017) Text in Ukrainian available at: https://www.ua.censor.net.ua/resonance/446561olova_departamentu_kiberpolitsiyi_sergiyi_demedyuk_proty_ukrayiny_vedut_tsilespryamovanu_kiberviyinu.

[25] Materials of the Single State Registry of Court Decisions of Ukraine: http://reyestr.court.gov.ua/Review/65496457.

banking secrets (art.231), its disclosure (art.232), acquisition, selling or using specialized technical means of gathering information (art.359). In practice, such acts are either qualified as multiple offences or, by attributing more value to the subjective elements—as the non-Chapter XVI offence.

Computer-Related Offences The Convention establishes obligations to criminalize only two of such crimes: computer-related forgery and computer-related fraud. From the wording of its art.7 and art.8 it can be seen that the key feature that allows to separate these computer-related crimes from their "traditional" counterparts is that the former are conducted through "input, alteration, deletion, or suppression of computer data" or through "interference with the functioning of a computer system". Based on these particular characteristics, it is possible to substantially broaden the list of crimes that fall into this category. That said, it is quite hard to establish a finite number, since the combination of the rapid technological development and the inventiveness of the criminal mind can always bring something new to the table.

The responsibility for cyber fraud is prescribed by art.190 p.3 of the Criminal Code of Ukraine: fraud that is carried out through means of illegal operations with electronic-computational devices. A related offence is that of art.200—illegal activity with transfer documents, cards and other means of access to bank accounts, electronic currency, and equipment made for their manufacture. The Code, however, does not explicitly establish responsibility for cyber forgery, allowing it to be qualified under the same articles[26] as its traditional counterpart.

> An example of cyber fraud can be seen in another relatively recent case, where a group of criminals from Yuzhnoukrainsk (Mykolaiv Region), created at least 10 online-shops on web-platforms such as «zakupka.com», «etov.ua», placed ads about selling mobile phones, motherboards and other items that they didnot possess and didnot have an intent to sell. The perpetrators asked for full payment upfront and used intermediaries who would receive the money and forward it to them (According to the information of the Cyberpolice website).

A separate group of offences that can theoretically be allocated into the category of computer related is connected with the provision of illegal services through cyberspace, for example gambling (art.203^2) or selling narcotics (art.307). Furthermore, as demonstrated by the high-profile incidents connected to the energy sector or some of the objects harmed by the Petya infection (such as the radiation monitoring systems at the former Chernobyl nuclear power plant), cybercrimes may share characteristics with acts of terrorism (art.261) or attacks on objects that have items posing an elevated danger for the environment (art.258), as well as other similar crimes that cause a common danger. The Code, however, does not contain special clauses with regard to committing these crimes through the use of computers and networks.

Content-Related Offences The Budapest lists two types of such offences: those related to child pornography and those related to infringements of copyright and

[26] Depending on the type of forged document: art. 205^1, 216, 223^1, 224, 318, 358, etc.

related rights. The Criminal Code prescribes liability for distribution of pornographic materials, including that involving minors (art.301). The Code also establishes liability for violation of copyright and related right (art.176) and for violations of other intellectual property rights (art. 177, 229, etc.) that can be carried out with the utilization of computers and networks.

> One example is a recent copyright infringement case (art.176). Odessa Regional Cyberpolice apprehended the establisher of an online-resource „icinemax.net" and stopped its functioning. The resource distributed pirated video content. The damage is estimated to be more than 3 000 000 UAH. (approx. 95 000 EUR) (According to the information of the Cyberpolice website).

> A more disturbing example of a content-related offence is related to child pornography distribution (p.4 art. 301). The Kyiv Department of Cyberpolice together with investigators of one of the capital's regional departments apprehended a person that was distributing child pornography over the Internet from her PC. To make things worse, the authorities state that in the past she had worked as a schoolteacher! (According to the information of the Cyberpolice website)

Acts of a Racist and Xenophobic Nature Committed Through Computer Systems This category of offences was introduced by the 2003 Additional protocol[27] to the Convention. It consists of dissemination of racist and xenophobic material through computer systems; racist and xenophobic motivated threats, insults; denial, gross minimization, approval or justification of genocide or crimes against humanity. Responsibility for said crimes is mostly established in the Criminal Code of Ukraine: e.g., art.161—violation of equality of citizens (including insults and threats) based on their racial, national background, religious beliefs, disability and other grounds, art. 300 importation, creation or distribution of works that propagate a cult of violence and cruelty, racial, national or religious intolerance and discrimination, art.442 p.2—public incitement to genocide and creation/distribution of respective material.

Although no specific "cyber" clauses are present in the articles, the wording allows qualification of acts committed through computers/networks to be qualified as such either independently or as multiple offences. However, some of the characteristics of the crimes in the Criminal Code do not seem to correspond with those of the Convention; furthermore, not all criminal activity listed in the Protocol appears to be criminalized by Ukrainian legislation. At the same time, this possible discrepancy is not the focus of this publication; therefore, it is left open to future specialized research.

Investigative Jurisdiction A natural question here is the separation of jurisdiction between the National Police and the Security Service in dealing with the above-mentioned crimes. The answer lies in the provisions of art.216 of the Code of Criminal Procedure. By default, all crimes fall under the jurisdiction of the police investigators. The Service, however, is tasked to investigate the cybercrimes

[27] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg, 28.1.2003.

connected to treason, espionage, terrorism, disclosure of state secrets, gathering or transmitting information gathered in the course of investigative, counterintelligence activity, in the sphere of state defense, of military information, acquisition, selling or using specialized technical means of gathering information. However, due to difficulties of qualification of these relatively new categories of crimes,[28] there is high potential for jurisdictional conflicts, a factor that is prone to reduce the effectiveness of this particular area of cybersecurity.

5.3 Investigative Powers

As was noted above, one of the key functions of law-enforcement bodies is the investigative function; therefore, we should overview their investigative powers, focusing on those that can be most relevant with regard to cybercrime.

The Code of Criminal Procedure provides for two categories of investigative activity: investigative actions (ch.20) and covert investigative actions (ch.21). Do note that if the actions of a law-enforcement officer overstep the legal requirements, leading to substantial harm, such an officer can be prosecuted under art.365 of the Criminal Code (abuse of power by a law-enforcement officer).

Investigative actions are supposed to be carried out in the presence of the person whose rights are being (lawfully) infringed, after informing them of their rights and obligations. Those actions that can apply to our area of interests may include interrogation, presentation of a person or object for recognition, search of property (carried out on the basis of a decision of an investigative judge), inspection (area, property, objects, or documents), investigative experiment, examination of a person, carrying out an expert examination.

Covert investigative actions, however, seem to be something more directly linked to counteracting the crimes that are discussed in this part of the article. The information about the fact of the conduct of such actions and their methods is by default non-disclosed. They are to be carried out only if the information about the crime or the perpetrator cannot be attained in another way. With some exceptions, (e.g., art.250 of the Code of Criminal Procedure—imminent danger to lives, etc.) they are to be sanctioned by an investigating judge.

One of the most noteworthy actions is interference in private communication (art.258) which includes audio and video control; arrest, inspection and seizure of correspondence. Another relevant one is interception of information from telecom networks, which is prescribed by art.263, defining it as application of technical surveillance means to select and record the content of information that is transmitted by a person; receiving, converting and recording various signals that are transmitted by communication channels. Furthermore, p.4 of art.263 states that the managers and employees of telecom operators are obliged to facilitate such interception of information from telecom networks, implement measures towards non-disclosure of the actions and the information that is received, to preserve the information. Apart

[28] Pointed out, for instance by Glib Pakharenko in "Cyber Operations at Maidan" (p.60): "the ultimate responsibility for cyber crimes has never made explicit, and in this regard there has been competition between the MVS and SBU", meaning the Ministry of Internal Affairs and the Security Service of Ukraine (Pakharenko 2016).

from that, it seems interesting to point out the action of acquisition of information from electronic information systems, established in art.264, which defines it as searching, identifying and recording data that is situated in an electronic informational system. Other noteworthy types of covert investigative actions include establishment of the location of a radio-electronic device (art.268); surveillance of a person, location or object (art.269); monitoring of bank accounts (art.269-1); audio/video surveillance of a location (art.271), etc.

5.4 Potential Improvements

At the same time, the capacity of law enforcement to affect cybercrime in Ukraine can be enhanced. First of all, the jurisdictional overlap that was pointed earlier in this section is indubitably a negative factor. It can be overcome by adopting changes to procedural law directly with regard to matters of jurisdiction as well as to substantial law, connected to clarification of the features of cybercrimes that will allow the qualification of acts as concrete crimes to be carried out without doubt. To a certain extent, the jurisdictional conflict may be also resolved by differentiating criminal responsibility for cybercrimes carried out against state and other information resources, objects of key infrastructure and other objects and a respective differentiation of jurisdiction. This particular measure will also allow differentiating the penalty in accordance with the degree of danger of the acts, therefore, implementing the principle of proportionality of punishment.

Other challenges related to law-enforcement bodies' capacity lie in their somewhat underdeveloped investigative powers. An analysis of the regulations in the area of cybersecurity allows pointing out possible developments. They are connected to: procedural mechanisms related to acquisition of electronic evidence, methods and means to identify and fixate cybercrimes, carry out expert examinations; mechanisms of carrying out urgent real-time procedural actions with the use of electronic documents and electronic digital signatures; establishment of a special procedure of interception of information from telecom channels when investigating cybercrimes; enforcement of the obligations of telecom providers and operators to record and store content and/or traffic data.

Apart from that, Ukraine should focus on developing the capabilities of law-enforcement bodies, in particular through improving their cooperation in accordance to joint action protocols, bolstering their response speed, training of all actors of the criminal justice system to operate with electronic evidence and to carry out their functions when dealing with the special features of cybercrimes.

6 Policy Measures

As was noted earlier in the article, establishing an efficiently functioning system of cybersecurity requires not only the employment of capabilities of various actors but also the drafting and implementing of a variety of sectoral policy measures. A list of such measures is presented in art.4 of the Strategy of Cybersecurity.

6.1 The principles

Before an overview of the measures is presented, it is sensible to have a look at the guiding principles that should be upheld during the designing and enforcement of the measures. Such principles are enshrined in para. 11–20 of art.1 of the Strategy. It seems possible to group them into three following categories.

Principles Monnected to Free Access to Cyberspace and Protection of Rights include openness, accessibility and protection of cyberspace; the rule of law and respect to the rights and liberties of persons and citizens; provision of democratic civil control over military and law-enforcement bodies that act in the area of cybersecurity.

Principles Connected to the Systemic Approach are those that point out the diversity of cybersecurity measures and define some of their features. They include proportionality and adequacy of measures to real and potential risks; priority of preventive measures; imminence of punishment for commission of cybercrimes; state-private partnership; priority of development and support of national scientific, technical and industry potentials.

Principles Connected to International Cooperation include said cooperation; development of common approaches in cyber threat counteraction; consolidation of efforts in investigating and preventing cybercrimes, deterrence of the use of cyberspace in illegal and military purposes; upholding the national interests of Ukraine.

This last group requires further elaboration. A number of national security threats, including those to cybersecurity, are connected to the conflict with the Russian Federation. References to this can be seen in a variety of normative documents in the given area. For instance, the Strategy of National Security (para.3 art.1) stipulates that one of the needs for the drafting of the Strategy is "the Russian threat that has a long-term character" as well as several other, stronger statements about the acts and intentions of the Eastern neighbor. The Cybersecurity Strategy also speaks of "the persisting aggression of the Russian Federation" (para.4 art.1) as a reason of the Strategy's enactment and "a wide, even dominating presence of organizations … directly or indirectly connected with the Russian Federation in the informational infrastructure of Ukraine" (para.2 art.2) that enables threats to cybersecurity. Even more is said in the Concept of Development of the Security and Defense Sector of Ukraine (CDSDS); one can turn to its provisions for further details.

A young state in today's world must look for inter-state cooperation in all areas of its functioning; defense and security are no exceptions. An understanding of this and, naturally, the above-mentioned problem, together with the desire to establish and uphold European values, inevitably drive Ukraine towards enhanced cooperation with the EU, with NATO and with the international community as a whole. Indicators towards this can be seen in the Strategy of National Security, which amongst other instances, in para.5 art.1 acknowledges that it is to be carried out in light of the implementation of the Association Agreement between the EU and Ukraine. The Cybersecurity Strategy, in turn, states that it is based on the principles of the Budapest Cybercrime Convention and, moreover, provides for various

directions of cooperation with NATO and EU. This vector of external politics is actualized even further and in more detail in the provisions of the CDSDS.

It is also worth to note that such cooperation, particularly in the area of cybersecurity, is mutually beneficial. The notion that cyberthreats pose a common danger for both Ukraine and the EU was recently confirmed by Hugues Mingarelli,[29] the head of the EU Delegation to Ukraine. Furthermore, benefits of cooperation in the area can be somewhat attributed to the following considerations. As noted by V.B. Khlevitsky, Ukrainian information infrastructure can be used a "transit base" for carrying out cybernetic attacks against third states (Хлевицький 2016, p.72)[30] including EU members. Furthermore, V. Prokhorenko spoke of a "possibility, that if cybercrime is "pushed out" of Europe, it will move to Ukraine".[31] If such movement manifests in the relocation of criminals or their bases of operation, it does not mean that they will stop targeting victims in Europe, it means that they will commit crime from a state where they can avoid EU prosecution with more ease. Therefore, without a common cybersecurity policy between the EU and Ukraine, these factors will still pose their respective threats to Union states. After all, geographical borders do not mean too much for criminal activity of the given area.

At the same time, the principles of this group should go hand in hand; the principle of "provision of national interests of Ukraine" should not be forgotten. Ukraine aims to establish itself not only as a strong independent state, but also as an equal, contributing, democratic member of the international community. In this regard, it is possible to quote D. Dubov, who writes, "Ukraine aims to be not merely an object, but also a subject of global politics, it has to form its own integral strategy regarding cyberspace" (Дубов 2014, p.219).[32] Therefore, when engaging in international cooperation and taking on international law obligations, Ukraine should not rush "head first", happily accepting all offers. It should carefully evaluate which deals and to what extent are aligned with its national interests, it should attempt to take initiative in drafting proposals, it should be more proactive and assume more responsibility in shaping its present and future.

6.2 The Directions

Having overviewed the principles, we may move on to the measures themselves. Do note that Ukraine is in the relatively early stages of establishing its system of cybersecurity (that said, so are most states), so the measures listed in art.4 of the Strategy represent a very ambitious "road map" that seems to be designed not just

[29] See the press release on the meeting between Turchinov (the CNDS Secretary) and Mingarelli on the CNDS website: http://www.rnbo.gov.ua/news/2826.html.

[30] Хлевицький В.Б. Окремі проблеми правового забезпечення кібернетичної безпеки в Україні в умовах розвитку інформаційного суспільства. P.72.

[31] Quoted by Badyuk M.O. and Foros G.V. Бадюк М.О., Форос Г.В. Деякі аспекти щодо проблем запобігання та протидії кіберзлочинності. P.175.

[32] Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва. P. 219.

for years, but perhaps even decades. In any case, the Strategy's article divides the measures into five categories.

Development of a Safe, Stable and Resilient Cyberspace This can be seen the broadest area of improvements, all measures here are of general organizational nature. Still, it is possible to note some concrete patterns. First of all, this area includes drafting and implementation of: general cybersecurity and cyberspace development policies, normative and terminological bases; harmonization of documents in the areas of electronic communication, information security and cybersecurity. Furthermore, this has to be carried by attaining compliance with international, EU, NATO standards; the need to take part in international cooperation including OSCE initiatives is also underlined. Another group of measures is connected to scientific and technological policies: development of electronic communication infrastructure, technologies of cyberprotection of mobile devices, of hardware and content security, security of applications and communication services, systems of technical and cryptographic protection of information. These measures, as well as some others, have to be carried out with the involvement of the expert potential of scientific facilities, professional and public associations. Yet another group of measures of this category seems to be economic regulatory: formation of a competitive environment in the area of electronic communication, information and cybersecurity services; creating the conditions for the introduction of modern technologies of cyberprotection in Ukraine. Moreover, the category includes measures of monitoring and reactive nature: development and improvement of the systems of state control of the level of information protection, independent auditing of information security, development of a network of response teams for computer emergencies, creation of a system of early detection, prevention and neutralization of cyberthreats. Finally, the category also lists measures of social outreach: increasing the level of "digital awareness" of citizens and the culture of secure behavior in cyberspace, of skills and abilities that are necessary for cybersecurity; implementation of state and public projects aimed at raising awareness about cyberthreats and cyberprotection; carrying out "drills" on emergencies and incidents in cyberspace.

Cyberprotection of Sate Information Resources and the Information Infrastructure that Processes Restricted Information This category composes mostly of technical measures that include: creating and ensuring the functioning of a national telecom network (a single platform of protected electronic communications of state authorities); a secure, integrated system of electronic state registries, databases, datacenters, including a single data center of backup storage of information of state electronic informational resources; improving the systems of storage, transfer and processing of state registers and databases; deployment of a single system of situation centers of bodies of the Sector of Security and Defense on the basis of a secure information infrastructure; introduction of an organizational-technical model of the national system of cybersecurity, operative reaction to cyberattacks and cyberincidents; development of new methods of prevention of these threats, spreading information about such methods. Furthermore, the category includes such measures as the development of requirements (normative) with regard to secure Internet usage and provision of electronic services by state bodies; increasing the

awareness of employees of state bodies involved in information and cybersecurity, carrying out respective trainings, etc.

Cyberprotection of Key Infrastructure The measures related to cyberprotection of key infrastructure include two groups. The first is connected to the development of a normative framework that regulates: the main principles of such protection, establishment of the criteria of key infrastructure; forming and establishing the functioning of a state registry of key infrastructure objects; drafting specific regulations for the cyberprotection of said objects; establishing qualification requirements and mandatory periodical certification for staff members that service them. The other group is directed at enhancing private–public cooperation in this area: organizing such cooperation, development of state-private partnership in preventing cyberthreats, reacting to cyberattacks and cyberincidents, neutralizing their consequences; developing of a mechanism of exchange of information on cyberthreats towards key infrastructure between the state, private sector and citizens; creation and assurance of functioning of cyberprotection units in these objects.

Development of the Potential of the Sector of Security and Defense in Regards to Cybersecurity A variety of measures are to be carried out by the subjects of the sector. These measures mainly involve military and intelligence bodies; however, some involve the National Police and the Security Service. The CDSDS provides further details in this regard. One group of measures is connected to enhancement of the capacity to manage high-profile threats: "cyberagression", cyberterrorism related to state electronic information resources, key infrastructure, hostile intelligence-subversive activity in cyberspace; creation of a single Armed Forces cybersecurity unit; development of the cybersecurity units of the other subjects of the Sector to comply with the standards of respective units of NATO members; enforcement of cybersecurity of technological processes in objects of key infrastructure; monitoring of the national cybersecurity system, development of sectoral indicators of cybersecurity. Another group of measures is directed at limiting the role of organizations that are under Russian Federation influence in taking part in information security and cybersecurity, limiting the usage of their products, technologies and services in the given areas. Furthermore, this category prescribes for modifications in criminal law, connected to: differentiation of criminal responsibility for cybercrimes carried out against state and other information resources, objects of key infrastructure and other objects; respective differentiation of jurisdiction. Lastly, the category includes measures of scientific and educational natures: development and coordination of research in the area of cybersecurity and cyberprotection for the purposes of national security and defense; development of a system of professional training for staff of the Sector, etc.

Fighting Cybercrime An important point is to be restated here: note that "fighting cybercrime" is seen as just one of the categories of cybersecurity policies of a state, further providing perspective on its limited place in the system of cybersecurity as well as on the place of cybercrime in the multitude of cyber threats. As to the measures of the category, it is possible to begin with stating the organizational ones: establishment of a protocol of joint action of law-enforcement bodies for fighting cybercrime, increasing the speed of response of such bodies (especially regional), creation of an effective and

convenient contact center for communicating about cybercrime.[33] Another group consists of normative changes aimed at the development of investigative powers: improvement of procedural mechanisms related to acquisition of electronic evidence, methods and means to identify and fixate cybercrimes, carry out expert examinations; regulating the question of the possibility of carrying out urgent real-time procedural actions with the use of electronic documents and electronic digital signatures; establishment of a special procedure of interception of information from telecom channels when investigating cybercrimes; enforcement of the obligations of telecom providers and operators to record and store computer data, traffic data. Furthermore, some measures, such as developing the procedure of blocking an identified informational resource (or service) by telecom operators and providers based on a court decision, seem to be aimed at improving the sanctioning options of criminal law. Finally, this category includes measures of professional development: preparation of judges (and investigative judges), investigators and prosecutors to work with electronic evidence, taking into account the particularities of cybercrimes; general elevation of the qualification level of law-enforcement bodies' operatives.

7 Perspective Areas and Recent Developments

7.1 The Challenges

As was noted in the beginning of the previous section, the complete list of policy measures of art.4 of the Strategy is aimed at years if not decades. Instead, it seems interesting to have a look at the priority cybersecurity measures that have to be adopted by Ukraine in the near future. A system of such measures can be found, for instance, in the CNSD Decision on the Treats to Cybersecurity of the State and Immediate Measures of their Neutralization[34] that was briefly mentioned in the

[33] Some steps in this direction have already been made. The website of the Department of Cyberpolice has an application form for reporting cybercrime https://cyberpolice.gov.ua/declare/. At the same time, we should assume that there should be a single contact center, however the CERT-UA's website also has a form for reporting cyberincidents http://cert.gov.ua/?page_id=295. The existence of duplicate contact centers creates certain doubts on the effectiveness of the system as well as demonstrating some institutional competition.

[34] After the submission of this article for peer review, the CNDS adopted a follow-up decision "On the state of execution of CNDS Decision of 29.12.2016 "On the Treats to Cybersecurity of the State and Immediate Measures of their Neutralization"…" (Decision of July 10, 2017, enacted by Presidential Decree of August 30, 2017 № 254/2017). Its adoption seems closely connected to the Petya incident. The majority of the provisions of the new decision refer to administrative and technical measures that detail the provisions of the original decision, with a focus on strengthening the protection of systems and networks of state bodies and state-owned enterprises as well as key financial institutions. Furthermore, the SSSCIP's regulatory authority is to be further expanded and its technical capacity is to be modernized. Apart from that, the new decision requires establishing an outsourcing mechanism of certain cybersecurity tasks to private entities within the framework of public–private partnership (art.1.4.). Furthermore, art.6 provides for immediate "activation" of international cooperation by the Security Service of Ukraine, the National Police and the SSSCIP. Finally yet importantly, in the area of criminal law, the decision (art.1.6 "Б") stipulates the drafting and submission to the Parliament of a law on differentiation of responsibility and investigative jurisdiction in regards to cybercrimes committed against state and other informational resources, objects of key informational infrastructure and other objects.

beginning of the article. It prescribes the implementation of a list of measures and sets various time frames (up to a year) for their enactment. Unfortunately, since the decision has been in force for more than half a year, it seems that the authorities are failing to meet many of them. However, it is necessary to clarify that the aim of this part of the publication is not to evaluate the implementation of Ukraine's policies in detail, rather to identify its next steps.

The measures prescribed by the Decision can be divided into several categories. An interesting point to be made is connected to para.3 and para.4 of the Decision that are "secret", *i.e.,* not available to the public. Apart from giving a certain understanding about the particularities of drafting an area-specific national security policy, this fact may also be inconsistent with the aforementioned principle of democratic civil control over cybersecurity. However, as was stated, detailed evaluation is not the goal here; therefore, we proceed with the groups of measures.

Legislative (Regulatory) Activity. The first category of measures consists of drafting and submitting legislative and regulatory acts for adoption. This task is set mainly before the Cabinet of Ministers. The acts to be drafted can be, in turn, divided into three groups. The first is directly connected to protection of key infrastructure: regulating the conditions of cybersecurity of objects of key infrastructure, the rights and obligations of cybersecurity subjects and owners (managers) of the objects; setting the mechanisms of interaction between these parties in cases connected with cyberattacks and cyberincidents; establishing of a concrete protocol of joint action[35]; establishment of limitations towards the use of software and telecom devices of organization of the "aggressor-state" on objects of key infrastructure[36]; forming the list of information-telecom systems of objects of key infrastructure of the state. The second group is connected to the prescription or increase of responsibility for violations in the area of cybersecurity: prescription of responsibility for violation of regulations on protection of key infrastructure; increase of responsibility for violating legislation connected to information protection in informational-telecommunication systems and non-compliance with the requirements of officials of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP); establishment of responsibility for non-compliance with the requests of officials of the Security Service of Ukraine (SSU).

The final group is measures that are aimed at attaining compliance with the Budapest Cybercrime Convention. Although the Convention was initially signed by Ukraine in 2001, ratified in 2005, with changes into the ratification law made in 2010, the state and level of the implementation of its obligations are incomplete. Among the implementation measures pointed out by the Decision are those that are to provide law-enforcement bodies with the authority to order owners of computer data (telecom operators and providers, other legal or natural

[35] Although, according to aforementioned official reports, a certain protocol was enacted in response to Petya, recent legislative or even regulatory acts do not contain it, therefore it is assumed that these are still prospective measures.

[36] This has been carried out to a certain extent, as briefly discussed later in the "special sanctions" section.

persons) to immediately record and store computer data necessary to solve a crime; establishing a set procedure to issue such orders; requirements towards telecom operators and providers to provide information to law-enforcement bodies (at their request), which is necessary to identify suppliers of services and the routes via which information was transferred; establishing the possibility to issue a court order to block (or limit) an identified informational resource (or service) by telecom operators and providers; establishing an effective mechanism of utilization of electronic evidence (gathered in the course of investigative activity) in criminal procedure.

Development of Technological Protection This category includes measures that are aimed to enhance the technical aspects of national cybersecurity. Amongst them are: creation of main and backup protected data centers of storage of information and data of state electronic informational resources; creation and deployment of a national telecom network, connecting information-telecom systems of state bodies and state-owned companies to it. Other measures the effect of which can indirectly impact technological protection are: production of solutions to stimulate Ukrainian software to fulfill the needs of state bodies and state-owned companies; drafting a mechanism of additional work motivation for cybersecurity specialists of the sector of security and defense of Ukraine.

Financial Sector Security Several measures are aimed at enhancing security in the banking and financial spheres. Tasks of this category are mainly set in front of the National Bank that, however, has to work on them together with the SSU, the SSSCIP and the National Police. They include establishment of a legal mechanism of blocking the functioning of electronic payment systems of the "aggressor-state" on the territory of Ukraine; as well as drafting proposals of improvement of regulations on the protection of the information in informational-telecom networks of banks and other financial institutions.

Implementation of the National Program of Informatization [37] The program lists a system of tasks aimed at the development of a modern informational infrastructure of Ukraine. To be more precise, according to the provisions of art.2 of the law that regulates it: it is a complex of informatization projects that have a goal of creation, development and integration of information systems, networks, resources and information technologies or acquisition of means of informatization in order to support the functioning of state bodies, as well as other organizations. The areas of the regulation that the provisions of the program touch upon are much wider than the risk-management function of cybersecurity. Therefore, we will not overview the program in detail, leaving it for a more specialized research. What is important to note is that the program was originally adopted in 1998 and although several changes to it have been made over the years, they do not seem to be correspondent to the recent initiatives in the general area of national security or cybersecurity. Therefore, the Decision, perhaps guiding itself by the understanding of this, stipulates to adopt new measures connected to the implementation of the program, namely: development of new tasks of the program for 2018–2020; inclusion of said

[37] Regulated by Law On the National Program of Informatization of 04.02.1998 № 74/98-BP.

tasks together with a concrete roadmap of measures into the submission of the draft law On the State budget of 2018; establishment of a General state charterer[38] taking into account the current cybersecurity threats.

7.2 The Achievements

If the several last pages left the reader with the impression that Ukraine still has a titanic amount of work to carry out with regard to forming an efficient system of cybersecurity, then they have reached their goal. However, several things need to be made clear in relation to this. Once again, it is necessary to restate that most of the world powers, states with much more developed legal systems and level of technological development are also in the early stages of formation of their systems of cybersecurity and also require tremendous efforts to develop them. Furthermore, the fact that much needs to be done should not diminish the achievements of Ukraine in the given area.

The Basic Regulatory Framework First of all, it is important to place focus on the adoption of a series of normative documents that establish the basic framework of the system of cybersecurity that has been carried out during the last several years. Among them are the Strategy of National Security; naturally, the Cybersecurity Strategy; the Concept of Development of the Sector of Security and Defense; enactment of the Regulation on the National Coordination Center of Cybersecurity;[39] making changes into the Law "On the State Service of Special Communications and Information Protection of Ukraine" that among others, created a legislative basis for the functioning of the cyberthreat response team CERT-UA within the structure of the Service;[40] enactment of the Order of Formation of the List of Information-Telecom Systems of the Key Infrastructure of the State;[41] adoption of the aforementioned CNDS Decision On the Threats to Cybersecurity of the State and Immediate Measures of their Neutralization, as well as a number of others.

The Special Sanctions A relatively recent development that requires some attention is connected to sanctions directed at physical and legal persons related to the Russian Federation according to a series of CNDS Decisions "On the Prescription of Personal Special Economic and Other Restrictive Measures (Sanctions)".[42] Although the measures are, to an extent, an economic retaliation in response to the conflict, they also serve another goal, directly related to the given field of research. The restrictions are aimed to fulfill the developmental directions of the Strategy of Cybersecurity as well as of the above-mentioned Decision on the

[38] Art.10 of the Law defines this as a respective state executive body that charters the Program's projects.

[39] Enacted by Presidential Decree of June 7 2016 № 242/2016.

[40] Law № 1194-VII of April 4, 2014.

[41] Cabinet of Ministers Resolution of August 23 2016. Provides several interesting definitions such as "cyberattack", "key infrastructure" and objects of thereof. It also prescribes for the actual formation of the list of such objects, however, this has not been carried out.

[42] Enacted by Presidential Decrees of September 16 2015 № 549/2015, of October 17 2016,№ 467/2016, of May 15 № 133/2017, etc.

Threats to Cybersecurity of the State and Immediate Measures of their Neutralization with regard to limitation of Russian software in Ukrainian information systems and networks, including that of antivirus software developing companies Dr.Web and Kaspersky Lab. The latest development took place on May 15, 2017, when Presidential Decree №133/2017 enacted such sanctions with regard to popular social networks VKontakte and Odnoklassniki, the highly used Mail.ru service as well as most of the services provided by Yandex. The impact of this measure is to a certain extent controversial. Naturally, the restrictions potentially had a direct positive impact on cybersecurity; furthermore, they seemed to have stimulated Ukrainian software producers who saw a new niche in the market (Литвинова 2017),[43] thus also fulfilling the policy goals of supporting national developers. At the same time, the popularity of the resources that have been blocked[44] could not have made the measures be met with arms wide open by all of the population, as more and more people find ways to gain access to the services, for example through use of VPN technologies.[45]

The Draft Law The draft law On the Fundamentals of the Provision of Cybersecurity of Ukraine (Draft law, 19.06.2015 №2126a) had been adopted after first reading on September 20, 2016 and was prepared for the second reading. On a hearing that took place April 7, 2017, the profile Committee on Informatization and Communication of the Parliament of Ukraine evaluated the draft and recommended its adoption in the second reading.[46] However, after a second reading that took place May 25, the Parliament decided to return the draft to the committee for further modifications before bringing it to another second reading in the future. Right now, it is impossible to accurately predict date (or fact) of final adoption.

As the reader may have noticed, the normative framework of cybersecurity of Ukraine is based mainly on acts of the regulatory and not legislative level. This seems to be a serious flaw with regard to the provision of one of important areas of national security. In this sense, the Draft Law seems one of the possible solutions to this matter. At the same time, after analyzing its text, one can conclude that it does not regulate all the cybersecurity questions in detail. At the same time, it is not its aim and, perhaps, it cannot even be a reachable aim within the contents of a single law. The draft is a legislative framework measure and it does, however, provide for the following.

One of its main achievements is the establishment of a vast terminological base on the legislative level. The importance of this has been pointed out earlier in the publication. It is also supported by opinions of other researchers, for instance D. Dubov, who wrote that "the efforts of the state in regards to developing an effective

[43] See article by P.Litvinova. Полина Литвинова. Как повлиял запрет российских сайтов на ИТ-рынок Украины.

[44] Ain.ua reported around 13 million Ukrainian VKontake users in 2014 and 2015 https://ain.ua/2015/09/16/ukraincy-vo-vkontakte-vozrast-mobilnost-dostatok-i-drugaya-statistika and 13 million users in 2014; RBK reported 18 million in 2017 https://styler.rbc.ua/rus/zhizn/vkontakte-ukraine-ustanovil-novyy-rekord-1495034924.html.

[45] Read further article by D. Kazanskiy. Денис Казанський Невіртуальний ефект. Наслідки блокування російських сайтів.

[46] See official website of the Committee: http://komit.rada.gov.ua/fsview/73002.html.

system of cybersecurity, should be concentrated particularly on defining and establishing on a normative-legal level the key terminology and definitions of the area of cybersecurity" (Дубов 2014, p.275).[47] Furthermore, R.V.Mukoida and A.O. Schelehov state "Ukraine in 2005 ratified the Cybercrime Convention, however the normative-legal base connected to ICT crimes is still imperfect… The law operates with concepts that are either not defined or their definitions in different acts are inconsistent" (Мукоіда, Шелехов 2016, p.36).[48]

The Draft Law attempts to bring such clarity and consistency by defining such concepts (art.1) as: cyberincident, cyberattack, cybersecurity, cyberthreat, cyber-protection, cybercrime, cyberspace, objects of key infrastructure, national electronic information resources, national telecom network, electronic communication network (communication system), system of management of technological processes (technological system).

Furthermore, the Draft provides for a legislative level establishment of fundamentals of the system of cybersecurity of Ukraine and its directions of development, principles of provision of cybersecurity, as well as its actors. Many of the Draft's provisions are similar to the norms of the Cybersecurity Strategy, but it is necessary to stress out that the Strategy is a regulatory-level instrument, the Draft will be a law, the first framework law in the area of cybersecurity.

A separate part of the Draft is connected to international cooperation. It is to take place in the forms of: cooperation with foreign states, their law-enforcement bodies and special services, international organizations that lead the fight with international cybercrime; prosecution on the territory of Ukraine of persons that committed cybercrimes abroad; joint cyberprotection measures including joint trainings (maneuvers) of the military, law-enforcement, special services, etc.; exchange of information.

Another aspect of the Draft is establishment of criteria for objects of key infrastructure and inclusion of a general provision of placement security obligations on the parties that carry out their management (art.6).

Finally, an important addition of the Draft is the framework regulation of state-private cooperation in the area of cyberspace (art.9). It is supposed to manifest in the creation of a system of rapid detection, prevention and neutralization of cybertreats, with the inclusion of volunteer organizations; increasing the level of "digital awareness" of citizens, implementing respective state and public projects; exchange of information about threats between state bodies, the private sector and citizens; partnership and coordination of cyberincident rapid response teams; involvement of the potential of experts, research facilities and professional associations into the development of cybersecurity projects; providing consultations and practical help in cyberincident response; measures of professional development of cybersecurity staff; establishment of a mechanism of public control of the effectiveness of cybersecurity measures.

[47] Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва. P.275.

[48] Мукоіда Р.В. Шелехов А.О. Законодавство України у сфері боротьби з кіберзлочинністю. P.36.

8 Summary of Findings

Understanding cybersecurity Challenges connected to cybersecurity regulation in Ukraine begin with its normative definition. Although it is defined in para.10 art.1 of the Strategy of Cybersecurity, as "…a condition of protection of vital interests of persons and citizens, society and state in cyberspace that is achieved by a complex utilization of a totality of legal, organizational, informational measures…", the concept has not yet founds its place in a legislative act. Furthermore, even the regulatory level establishes an uncertain correlation between cybersecurity and information security, attempting to set them as different categories. In turn, the author's analysis allows to state that at least on the level of regulatory acts, information security and cybersecurity are two spheres of national security that possess different defining qualities; thus, they cannot be neither subordinate nor alternative. Therefore, it is necessary to point out the flaw in the establishment of the borders of these spheres of national security in Ukraine, which exists on both the normative and theoretical levels and advocate the need of in-depth research of this question with a further goal of drafting and adopting a consistent legislative framework.

At the same time, it is possible to point out several key features of the approach of the Ukrainian state to cybersecurity. The first one is the definite understanding of the importance of the protection of interests connected to cyberspace by inter-alia setting out cybersecurity as one of the key spheres of national security. The second feature is connected to understanding cybersecurity as a threat-based, risk-management function. Finally, the third feature lies in the adoption of systemic approach to cybersecurity provision. Thus, it is understood that establishing a functioning framework of cybersecurity requires a coordination of different sectoral policies and employment of capabilities of various actors, both state and private.

The Threats The threat-based nature of the function of cybersecurity provision requires identification of the threats to this sphere of national security. During the last years, Ukraine has been faced with multiple actualizations of such threats. Among them are the recent spread of the Petya malware, WannaCry ransomware, the 2015–2016 attacks on the energy sector, the 2014 attack on the presidential election, various incidents related to information systems and networks of state bodies and state-owned companies in 2016, incidents connected to the Euromaidan in 2013–2014 as well as low-profile cybercrime that occurs on a day-to-day basis. From the given examples, one can see that threats can be of different nature, the results of actions of different actors that have different motives. They can be aimed at many objects, possess various magnitudes, create different victims and as a result —a multitude of harmful consequences. Accordingly, the qualities of each threat should be assessed, and a combination of measures and capabilities of various structures should be utilized as proportionate management mechanisms. This understanding is fully consistent with the systemic approach to provision of cybersecurity and further underlines its importance.

At the same time, a creation of "templates" of response mechanisms, tailored to types of threats, first of all requires the creation of a proper typology of threats, their

classification. Unfortunately, normative acts lack coherent classifications and the attempts of researchers are somewhat debatable. Inspired by the approaches of the EU Cybersecurity Strategy, the article presents an attempt to classify threats to the cybersecurity of Ukraine, dividing them into three broad categories: threats aimed at cyber defense actions directed at key infrastructure or informational resources (regardless of the actor, be it a hostile state, a "hacktivist" organization, a terrorist group, etc.); "generic" cybercrimes (crimes against confidentiality, integrity and availability information, computer-related and content-related offences, etc., however aimed mainly at interests of private entities and not the society in general) and threats to cyber resilience (non-intentional or completely force majeure cyberincidents).

The System of Actors The system of actors tasked with provision of cybersecurity of Ukraine can be divided into four basic pillars: defense and (counter) intelligence structures, law-enforcement bodies, technical protection regulators, the private sector and a coordinator—the National Coordination Center of Cybersecurity of the CNSD. The higher the profile of a threat actualization, the higher are the chances that various actors have to work together. Although during the latest incident connected to the "Petya" ransomware spread, various structures were cooperating under certain protocols recently developed by the CNDS, their contents are not made freely available to the public and, therefore, they cannot be evaluated.

Another important point with regard to the system of actors is the role of the private sector. In Ukraine, the area of public–private partnership is only at an early stage of its establishment: the legal framework of such cooperation is not fully developed. Furthermore, Ukraine is still lacking in terms of specialized research institutions that can contribute to cybersecurity provision. At the same time, it is worth to note that these problems are not intrinsic only to Ukraine—questions of the functioning of public–private partnership are debated even in states with the most advanced legal systems.

The Role of Law-Enforcement The previous section of the publication has partially illustrated the limitation of the role of law-enforcement bodies in the provision of cybersecurity of the state, law-enforcement can be seen as but one of four pillars on which the system stands. At the same time, as limited as it can be, it fills its key niche and must function to its full potential.

The main actors here are the Security Service of Ukraine (in its investigative capacity) and the National Police of Ukraine (more specifically, the Department of Cyberpolice). These structures are mainly tasked with counteracting various types of cybercrime: offences against the confidentiality, integrity and availability of computer data and systems (mainly Ch.XVI Special Part of Criminal Code), computer-related offences (e.g., cyberfraud—p.3 art.190; machinations with pay-cards—art.200, etc.), content-related offences (e.g., art.176, art.301, etc.), acts of racist and xenophobic nature committed through computer systems (e.g., art. 151, art. 300), as well as others. Unfortunately, difficulties in qualification of some of the mentioned acts, as well as other factors, create a basis for jurisdictional conflicts between the Security Service and the Cyberpolice, which definitely do contribute to effective cooperation and, therefore, this area can be seen as one that requires improvement.

When investigating cybercrimes, both the Cyberpolice and the Security Service are bound by the provisions of the Code of Criminal Procedure. Its norms grant the actors authority to carry out a variety of investigative actions (both overt and covert); however, some of their mechanisms could also be improved. They are, for example: carrying out urgent real-time procedural actions with the use of electronic documents and electronic digital signatures; establishment of a special procedure of interception of information from telecom channels when investigating cybercrimes; enforcement of the obligations of telecom providers and operators to record and store content and/or traffic data, etc. Please refer to the body of the article for further details of possible improvements to law-enforcement capacities/capabilities.

The Policy Measures Establishing an efficiently functioning system of cybersecurity requires not only the employment of capabilities of various actors but also the drafting and implementing of a variety of sectoral policy measures. According to the provisions of the Cybersecurity Strategy, these measures are to be employed in accordance with a set list of principles. It is possible to divide the principles into several categories, namely principles connected to free access to cyberspace and protection of rights, principles connected to the systemic approach and principles connected to international cooperation. Regarding the latter category, it is evident that the vector of such cooperation is based on today's external policy situation. At the same time, while enhancing Ukraine's cooperation with EU and NATO (which should be seen as mutually beneficial), sight of the national interests of Ukraine should not be lost and thus assumption of new international law obligations should be approached with care and much deliberation.

As to the measures themselves, it is not sensible to go over their categories here; one can refer to the respective part of the article. As a generalization, it is possible to state that they include a multitude of measures of legal and organizational nature, economic, technical, monitoring, research and scientific measures and those that are connected to different aspects of public–private partnership.

Recent and Perspective Developments Many of the above-stated policy measures represent the developmental directions that are to be implemented in mid to long-term timeframes. On the other hand, useful sources to analyze the short-term goals are the CNSD Decision on the Treats to Cybersecurity of the State and Immediate Measures of their Neutralization as well as the follow-up Decision regarding the execution of the former (see footnote 58 in 7.1). These measures can be divided into several categories: legislative activity (connected to regulation of the protection of key infrastructure, prescription of increase of responsibility for violations, attaining compliance with the Cybercrime Convention); development of technological protection; financial sector security measures; measures connected to the implementation of the National Program of Informatization.

At the same time, it is important to note the achievements of Ukraine in the incredibly challenging task of establishing its system of cybersecurity. Firstly, they are the adoption of a series of normative documents that establish the basic framework of the system including the Cybersecurity Strategy itself as well as a number of other acts. A relatively recent achievement is connected to limitation of Russian software in Ukrainian information systems and networks, although there are some challenging aspects to it. Finally, light should also be on the development of

the Draft Law On the Fundamentals of the Provision of Cybersecurity of Ukraine that had passed first Parliament reading and hopefully will be adopted in the nearest future, solving several problems and inconsistencies, pointed out in the article.

General Concluding Remarks Ukraine has already carried out many steps in establishing its system of cybersecurity. It has adopted a substantial number of acts designed to create a general normative framework, as well as to regulate different specific aspects of cybersecurity. Ukraine has identified the threats to the national interests in this area of national security, set out directions of future policy measures and established a circle of actors responsible for the provision of cybersecurity. Now it stands on the verge of a very important milestone, the adoption of the first framework law, specifically directed at the legal regulation of the cybersecurity system. This can be seen as the next step that needs to be taken right now. At the same time, much more needs to be done. Amongst other areas of necessary legal improvements are establishment of detailed regulation of key infrastructure protection, differentiation of responsibility for cybercrimes, attaining further compliance with the Cybercrime Convention, as well as drafting and implementing measures of organizational, economical, technical, etc. nature.

Furthermore, the author's analysis permits to present several generalizations that can be inferred from the example of Ukraine. First, it seems evident that provision of cybersecurity as well as provision of other spheres of national security are threat-based, risk-management functions. Since the threats to cybersecurity can possess various natures, objects, magnitudes and other features, their negation requires different management mechanisms, not a single instrument but a "tool-kit". This, in turn, creates the necessity of a systemic approach, built on coherent implementation of measures of various policies and utilization of capabilities of various actors including those of the military and (counter) intelligence sector, law-enforcement, technical protection regulators, as well as the increase of the participation of the private sector in the form of enhancement of public–private cooperation. Moreover, such a system naturally establishes its important functions for criminal law, however, at the same time, limits its role to their exercise. Thus, one should not equate provision of cybersecurity with cybercrime counteraction and place more obligations on criminal law or on law-enforcement bodies than they are able to fulfill, further blaming them for ineffectiveness, incompetence or corruption. If we follow that path, we are better of blaming ourselves for poor distribution of tasks between actors, for trying to screw in a nail with a screwdriver.

References

BBC (2017) Cyber-attack: Europol says it was unprecedented in scale. (13.05.2017). http://www.bbc.com/news/world-europe-39907965. Accessed 01 Aug 2017

Brandom R (2017) The Petya ransomware is starting to look like a cyberattack in disguise. (27.07.2017) The Verge https://www.theverge.com/2017/6/28/15888632/petya-goldeneye-ransomware-cyberattack-ukraine-russia. Accessed 01 Aug 2017

Business Censor (2017) A virus attacked computer systems of the Chernobyl NPP. (27.07.2017) (Text in Russian) https://biz.censor.net.ua/events/3028627/virus_atakoval_kompyuternye_sistemy_chernobylskoyi_aes. Accessed 01 Aug 2017

Carvalho H (2017) The preventive turn in criminal law. Oxford University Press

Dearden L (2017) Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers. (27.07.2017) The Independent http://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html. Accessed 01 Aug 2017

Dudley-Nicholson J, Bickers C (2017) Australian businesses warned as 'unprecedented' cyber attack hits Europe. (29.07.2017) News.com.au http://www.news.com.au/technology/online/hacking/cyber-attack-hits-europe-unprecedented-says-ukraine-prime-minister/news-story/f67abdaafb934aa23491ce9cffa44145. Accessed 01 Aug 2017

Gertz B (2017) Freighter was on autopilot when it hit US destroyer. (23.06.2017). The Washington Free Beacon. http://freebeacon.com/national-security/freighter-autopilot-hit-us-destroyer/. Accessed 01 Aug 2017

Goldman R (2017) What we know and don't know about the international cyberattack. (12.05.2017). The New York Times. https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html. Accessed 01 Aug 2017

Gorodnikov O (2017) Petya.A ransomware was a cover, the attack was planned for several months,—SSU and ESET. (05.08.2017) Tehnot. (Text in Russian) http://tehnot.com/virus-vymogatel-petya-a-byl-prikrytiem-ataka-gotovilas-neskolko-mesyatsev-sbu-i-eset/. Accessed 01 Aug 2017

GReAT (2017) WannaCry ransomware used in widespread attacks all over the world. (12.05.2017). Securelist. https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/. Accessed 01 Aug 2017

Koval N (2015) Revolution Hacking. In: Kenneth G (ed) Cyber war in perspective: Russian aggression against Ukraine, NATO CCD COE Publications, Tallinn

Nekrasov V (2016) Ukraine is losing the cyberwar (09.12.2016). Ekonomichna Pravda (Text in Ukrainian). http://www.epravda.com.ua/publications/2016/12/9/613957/. Accessed 01 Aug 2017

Nekrasov V, Polyakova A (2017) This is war: Ukraine was shaken by the largest cyberattack in history. (27.07.2017). Ekonomichna Pravda (Text in Ukrainian). http://www.epravda.com.ua/publications/2017/06/27/626518/. Accessed 01 Aug 2017

Pakharenko G (2016) Cyber operations at MAIDAN: a first-hand account. In: Kenneth G (ed) Cyber war in perspective: Russian aggression against Ukraine, NATO CCD COE Publications, Tallinn

Roth A, Nakashima E (2017) Massive cyberattack hits Europe with widespread ransom demands. (27.07.2017) Washington Post. https://www.washingtonpost.com/world/europe/ukraines-government-key-infrastructure-hit-in-massive-cyberattack/2017/06/27/7d22c7dc-5b40-11e7-9fc6-c7ef4bc58d13_story.html. Accessed 01 Aug 2017

Sieber U, Vogel B (2016) Terrorismusfinanzierung. Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht. Max-Planck-Institut für ausl. und intern. Strafrecht. Duncker & Humblot

TechToday (2017) The Petya 2.0 epidemic: simple extortion or an attack on a state? (04.07.2017). (Text in Ukrainian) https://techtoday.in.ua/reviews/epidemiya-petya-2-0-proste-zdirnitstvo-chi-ataka-na-derzhavu-75975.html. Accessed 01 Aug 2017

The Cyberpolice of Ukraine (2017) The Petya (Diskcoder.C) virus was the cover up for the largest-scale cyberattack in the history of Ukraine. (Text in Ukrainian) https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/. Accessed 01 Aug 2017

The Guardian (2017) British Airways cancels all flights from Gatwick and Heathrow due to IT failure. (28.05.2017). https://www.theguardian.com/world/2017/may/27/british-airways-system-problem-delays-heathrow. Accessed 01 Aug 2017

Ukrinform (2017) The Ministry of Defense has successfully repelled the cyberattack. (30.06.2017) (Text in Russian). https://www.ukrinform.ru/rubric-society/2256867-v-ukraine-sozdaut-kibervojska-poltorak.html. Accessed 01 Aug 2017

Zeit Online (2017) Britische Kliniken schicken Patienten nach Hause. (13.05.2017) (Text in German) http://www.zeit.de/digital/internet/2017-05/hackerangriff-deutsche-bahn-ransomware-weltweit. Accessed 01 Aug 2017

Бадюк М.О., Форос Г.В. Деякі аспекти щодо проблем запобігання та протидії кіберзлочинності//Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. 233 с

Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія/Д. В. Дубов. К.: НІСД, 2014. 328 с

Казанський Д. Невіртуальний ефект. Наслідки блокування російських сайтів. (08.06.2017) Тиждень.UA. (Text in Ukrainian) http://tyzhden.ua/Society/194070. Accessed 01 Aug 2017

Катеринчук І. П. Правоохоронні органи в боротьбі з кіберзлочинністю//Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. 233 с

Косаревська О.В. Новіцький О.І. протидія кіберзлочинності як складова інформаційної безпеки держави.//Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. 233 с

Литвинова П. Как повлиял запрет российских сайтов на ИТ-рынок Украины. (09.06.2017) 24 Канал (Text in Russian). http://24tv.ua/ru/kak_povlijal_zapret_rossijskih_sajtov_na_it_rynok_ukrainy_n827724. Accessed 01 Aug 2017

Мукоіда Р.В. Шелехов А.О. Законодавство України у сфері боротьби з кіберзлочинністю.// Кібербезпека в Украні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. 233 с

Парфило О. А., Нізовцев Ю. Ю. Актуальні питання судово-експертного дослідження шкідливих програмних засобів у межах протидії кібертороризму/О.А. Парфило, Ю.Ю. Нізовцев// Криміналістичний вісник 2016. № 1 (25), с. 79

Форос Г.В. Кондрашева К.С. Інформаційне суспільство та кібербезпека.//Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. 233 с

Хлевицький В.Б. Окремі проблеми правового забезпечення кібернетичної безпеки в Україні в умовах розвитку інформаційного суспільства.//Кібербезпека в Україні: правові та організаційні питання: матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. 233 с