РОЗДІЛ ІІ
Суспільні комунікації

УДК 327(4):351.746:007
Kyrylo Vetrov,
student of the Faculty of International Relations,
Lesya Ukrainka Eastern European National University
Yevhenija Voznyuk,
candidate of Political Sciences, Associated Professor,
Lesya Ukrainka Eastern European National University,
43024, Ukraine, Lutsk, Vynnychenka str., 28, office 205
Vozniukjane.vippo@gmail.com, Voznyuk.Yevhenija@eenu.edu.ua
ORCID ID https://orcid.org/0000-0002-7828-7430

INFORMATION TERRORISM AS A MODERN THREAT FOR INFORMATION SECURITY OF EUROPEAN STATES

We note that the effective and active struggle of European countries with information terrorism takes place within the framework of the European Union, all its member-countries, as well as neighboring countries and applicants for accession. Therefore, it should be stressed that the EU is pursuing itself a very active policy in the field of information security. At the moment, it brings together highly developed countries that have a tremendous impact on international relations by establishing norms and standards of conduct of states in the political, economic, social, informational and other spheres. The main objective of the EU is to strengthen the European Commission's dialogue with international organizations and partners on the issue of network security and, in particular, on the growing dependence on electronic networks. Political priorities in the field of information security, defined by the governing bodies of the European Union, are being implemented at the national level by both state authorities and non-governmental organizations.

Analyzing all the above, it can be concluded that within the framework of the EU, information security is considered, first of all, as a state of information networks and systems that provides an adequate level of protection of the integrity, availability, authenticity and confidentiality of information and the appropriate level of counteraction to external negative influences. Priorities of EU policy in the field of information security are the creation and implementation of programs and various technical means of protection of information and communication technologies; development of normative legal acts that establish a list of crimes in the IT sphere and criminal liability; ensuring a high level of public awareness of the risks, threats and ways of protecting their information systems / networks from undesirable effects.

Key words: *European states, European Union, cybersecurity, cybercrime, information terrorism, information security, ENISA.*

1. INTRODUCTION

Formulation of the Problem. The first strategies of cyber security appeared at the beginning of the last decade. One of the first states to adopt cybersecurity as a statelevel issue was the United States, where the National Security Strategy in cyberspace was published in 2003. After that, such Strategies and security plans in the virtual space have spread throughout Europe. For example, Germany adopted the State Plan for the Protection of Information Infrastructure in 2005. In 2006, a strategy to enhance Internet security in Sweden was developed. After a major cyber attachment in 2007, Estonia became a member of the European Union, and in 2008 it published a broad state strategy on cyber security. In the same year similar Strategies are being created in Finland and in Slovakia. List of all national cybersecurity strategies of the European Union and some other non-member countries, published by the European Network and Information Security Agency.

With a view to developing a new EU strategy on cybercrime, the European Commission in February 2013 proposed a directive on measures to ensure a high level of network and information security (NIS) throughout the Union. Due to the interconnection of network and information systems, significant failures in one Member State can affect other Member States and the Union as a whole.

2. RESULTS OF THE STUDY

The stability of network and information systems, as well as the continuity of core services, are essential for the proper functioning of the internal market, in particular, for the further development of a single digital market. This directive requires all Member States to create «Computer Emergency Response Teams» (CERT) and adopt national NIS strategies and plans for cooperation. As a major innovation, the proposed directive requires mandatory notification by market operators of incidents that have a significant impact on the security of key services [1].

CERT is the center for responding to cyber attacks. The Incident Response Team manages the handling of information security incidents within its organization or network. Their task is to prevent attacks and raise awareness among citizens, detect incidents to actual tracking and resolve incidents.

The European Commission’s policy on cybercrime is being implemented in four main areas. First, it is a law-making process. The most important legislative decision is the Framework Decision of the EU Council of Ministers on attacks on information systems from January 17, 2005. A framework decision is intended to ensure a minimum level of convergence of criminal law for the most common forms of criminal activity regarding information systems, such as unauthorized access, unlawful interference with the system and data.

Secondly, the European Commission encourages cross-border cooperation between law enforcement agencies of the EU member states through the organization of conferences, the creation of round-the-clock contact points in the EU member states, and the development of a platform for training experts in the field of combating cybercrime.

Thirdly, the European Commission is developing cooperation between the public and private sectors in the fight against cybercrime, in particular, cooperation between law enforcement agencies and private companies.

Fourthly, the European Commission encourages the signing by the member states and other countries of the Convention on Cybercrime, developed by the Council of Europe, and participates in international working groups [2].

It should be noted that in Germany in recent years, the level of cybercrime has risen sharply. In 2016, the number of criminal offenses committed using Internet technologies amounted to 82,649 cases, while in 2015, the police registered 45,793 cybercrime. At the same time, the data of criminal statistics indicate an increase in the rates of disclosure of similar crimes. In general, the number of detected violations of this type increased by 5,9 %, reaching a level of 38,7 %.

We also emphasize that in 2016 the number of crimes in the field of computer information (computer sabotage) increased by 25 % – 4422 were registered. The legislation of the Federal Republic of Germany refers to this sphere, for example, such crimes as DDoS attacks of hackers. Such cyber attacks can disable computer systems or networks. The level of disclosure of such offenses decreased by 4,6 %, dropping to 22,1 % [1].

As for France, its Defense Department also intends to further strengthen its protection against cyberattacks, given the events of the election race. It is no less than the US vulnerable to such cyberattacks by foreign powers. Only in 2016 the cybersecurity service repulsed 24,000 attacks on computer networks run by its agency. Over the past three years, the number of cyber attacks has doubled. The danger also threatens civil infrastructure – computer systems of electricity and water, health, transport, telecommunications. Hacker attacks also present a threat to the media and all French authorities

The French Defense Minister said that by the end of 2019, the number of cybersecurity experts in the defense system will double and reach 2,600, in addition to 600 computer experts [3].

The most resonant was the situation in Estonia. The cyberattack against it is a coordinated simultaneous attack by hackers on computer systems of state institutions of Estonia, which began on April 27, 2007 during the exacerbation of Russian-Estonian relations connected with the transfer of the monument to the Bronze Soldier in Tallinn. A coordinated attack on hackers has, for some time, broken websites of parliament, ministries, banking institutions, and the media. According to many observers and experts, this cyberattack was one of the best organized and massive in the history of the Internet.

The events unfolded in three waves: the first attacks were registered on April 28, the next, more powerful wave on May 4, and the most powerful third wave took place on May 9, 2007. Internet traffic from abroad has grown fourfold, which has made attacked sites inaccessible. Due to attacks, up to 90% of banking transactions in Estonia experienced processing difficulties or could not be completed normally. At peak, the maliciously crafted traffic reached 100 MB/s. For the attacks, the resources of the Storm network were used. Somewhat later, when the processes against the

participants of the mutiny in April 2007, BlackEnergy bots were used to attack the website of the publication delfi.ee [4].

With the onset of this cyber war, the Estonian side accused Russia of its organization, but later the Minister of Defense denied these allegations in the absence of evidence. In the same year, deputy of the Derzhavna Duma of Russia Sergey Markov at a press conference admitted that one of his assistants was still involved in the organization of cyberattacks in Estonia. In 2007, the leader of the popular movement in Transnistria, Konstantin Goloskokov, also recognized the involvement of this organization in the above-mentioned attacks. In response, Estonia proclaimed Sergei Markov and leader of the that movement Vasyl Yakimenko as non-grata. Since Transnistria remains unrecognized, no country in the world has had the opportunity to bring cyberattackers from the region to justice [5].

One of the biggest cyber attacks was WannaCry (also known as WCry, WCrypt, WannaCrypt, WNCRY, and WanaCrypt0r) – a computer virus that strikes Microsoft Windows operating system by encrypting files. The virus has attacked government and businesses since May 12, 2017. One of the first was attacked computers in Spain, later the virus spread to other countries. The computer also suffered from the virus. As of June 17, 2017, computers were infected in 150 countries, the number of infected computers has exceeded 500,000. The requirement to transfer money has been translated into 28 languages of the world.

The virus attacked computers running Microsoft Windows by encrypting user files, then displays a message about converting files with a proposal within 3 days to pay the decryption key in bitcoins in the equivalent of $ 300 to unlock the data. If the required amount does not arrive, the amount will automatically be doubled. On day 7, the virus will destroy the data.

The message is displayed in the language of the state where the PC is located: in the UK – in English, in Russia – in Russian, in Spain – in Spanish. The amount of redemption is the same everywhere. Tens of thousands of computers around the world are infected. In Spain, Telefónica, one of the largest telephone companies in the world (fourth in number of subscribers), was infected. In Russia, ministries, Sberbank and MegaFon were attacked. In Germany, computers were infected by the Deutsche Bahn.

Originally responsible for a hacker attack, the British edition The Telegraph named the Shadow Brokers grouping associated with Russian government structures. However, in June 2017, the British National Cyber Security Center (National Cyber Security Center) claimed responsibility for the attack on the DPRK. In December of the same year, the United States government issued its own findings that the responsibility lies with the grouping of the Lazarus Group, which is the DPRK government [6]. The probable loss incurred by WannaCry over the first four days has exceeded $ 1 billion, given the magnitude of the large, simple large organizations around the world [7].

Also, researchers found a new type of malware for Android, which serves to extract the crypto currency Monero. The work of these programs during the extraction of cryptography can damage the device physically. The fact is that the Loapi virus requires that it be granted administrator privileges. After that, he begins to

independently load various harmful modules. One of these modules uses a smartphone to get Monero tokens. It is this feature that can overheat your device due to the long processor operation at the maximum load. Two days after the infection in the test smartphone, the battery swelled overheating. There is no indication that a malicious program can be distributed through Google Play [8].

It should be noted that Ukraine has suffered from cyber attacks in 2017, in particular Petya Virus – a family of malware that affects computers running the Microsoft Windows family. Recall that cyberattacks on June 27, 2017 were Ukrenergo, Kyivenergo, Nova Poshta and a number of Ukrainian banks and the media [9].

In Finland on November 7, 2016, it became aware of a DDoS attack against unidentified information systems in one of the European countries. Among other things, this attack affected the systems of heating management and supply of warm water in two residential buildings in Lappeenranta, in the east of Finland. The mechanism of protection of the control system automatically restarted it as a result of a surge of traffic, which made the system unworkable. The attack lasted from late October to November 3, 2016. The affected control systems were owned by Valtia, and the air temperature in the city was below 0 ° C (to -7 ° C) [10].

In 2015, a cyberattack was discovered on the Bundestag information system; among other things, the computer was damaged by the computer of the Federal Chancellor of Germany Angela Merkel. The responsibility for the attack lies with researchers at the Russian group of cybercriminals, the Sofacy Group, also known as Pawn storm, which is believed to be linked with Russian intelligence services. The same group attempted to break the information systems of the Netherlands Security Council in order to gain access to information on the investigation of the MH17 flight. And in May 2016 an attempt was made to attack the postal system of the Christian Democratic Union – the political party of Angela Merkel [11].

The European Strategy for a Secure Information Society, adopted in 2006, addresses the fight against online crime. However, actions against private and stateowned IT systems in the EU member states have brought a new tint to the problem, demonstrating that online crime is a potentially new economic, political and military weapon. In this area, further work is needed to develop a comprehensive European approach, increase awareness and strengthen international cooperation.

The most advanced European countries in the field of information security are Estonia, France and Norway, which conducted series of laws and created world-class organizations to protect the country in the information space.

Estonia was one of the first countries to develop a national strategy for cybersecurity in 2008, after which an updated strategy for 2014 was published. The country also has a wide range of legislation covering information security and cybersecurity.

Estonia has a well-organized computer emergency response team in the system, CERT Estonia, headed by an information system authority. In addition to national authorities, it is also important that the NATO Cybersecurity Center is located in Estonia. Although no formal public-private partnerships exist, government agencies work closely with relevant private organizations [12].

Estonia is the best country for information security in Europe. Just like Georgia, Estonia has strengthened its intelligence committee after the attack in 2007. This included the implementation of an organizational structure that could quickly respond to attacks on official acts requiring all vital services to maintain a minimum level of work even if they were cut off from the Internet [13].

France has a national cyber security strategy since 2011, focusing mainly on defense and national security issues. The National Information Systems Security Agency (ANSSI) is a well-organized body specializing in information security and integrated with the Computer Emergency Response Team in the country, CERT-FR. The cybersecurity strategy contains recommendations for closer collaboration with the private sector, but this has not been a significant development. ANSSI has published secret security measures that make France one of the few EU countries that has adopted such a focused approach to cybersecurity management [12]. There is a large-scale of cyber security training in the country. ANSSI has published a list of recognized universities that provide accredited degrees on cybersecurity.

Norway has the third place in Europe with the highest figure in the legal sphere. In addition to cybersecurity laws, Norway also conducted a study on its cyber-security culture, including informing citizens about the extent to which they will participate in monitoring their online activities [13].

Norway also has a law on personal data protection and an information and cyber security law. The Norwegian National Cybersecurity Strategy 2012 and NorCERT, part of the Norwegian Security Authority (NSM), have been developed. It is the national center for cyber security in Norway and the National Emergency Response Team (CERT). They cope with heavy computer attacks on critical infrastructure and information. Their mission is to increase the sustainability of Norway in the digital sphere. At the international level, it is the Norwegian contact center for ICT threats and incidents in the field of cyber security [14].

The European Union is pursuing a very active policy in the field of information security. At the moment, it brings together highly developed countries that have a tremendous impact on international relations by establishing norms and standards of conduct of states in the political, economic, social, informational and other spheres. The main objective of the EU is to strengthen the European Commission’s dialogue with international organizations and partners on the issue of network security and, in particular, on the growing dependence on electronic networks. Political priorities in the field of information security, defined by the governing bodies of the European Union, are being implemented at the national level by both state authorities and non-governmental organizations [2].

Therefore, in order to provide information security, the European Network and Information Security Agency (ENISA) was set up on March 10, 2004, which aims to strengthen the capabilities of the European community, member states and the business community in the field of prevention and responding to issues related to information security.

The main activities of the Agency are: – provide advice and assistance to the Commission and Member States in the field of information security; – collect and

analyze data on security incidents in Europe and emerging risks; – develop risk assessment methods to enhance the EU's ability to respond to threats to information security; awareness raising and development of cooperation among different actors in the field of information security, in particular by encouraging interaction between the public and private sectors [15].

The Agency also assists the European Commission in its preliminary technical work to update and improve European legislation on network and information security [15].

In its activities, ENISA builds on annual work plans / programs that contain a list of key priorities and objectives and planned activities to achieve the objectives. Thus, in particular, the agency's work program for 2016 identifies the following strategic priorities: increasing the ability of European electronic networks to withstand external influences; development of cooperation between Member States in the field of information security; identification of new risks in the field of information security and the formation of mutual trust between stakeholders in responding to new risks.

Analyzing and exploring the development of cybercrime in Ukraine, one cannot miss the tendency of all the states, which is aimed at uniting efforts to counter this phenomenon. Ukraine has risen in the world ranking of countries with the largest number of cyber threats and for the first time entered the dozens of countries with the largest number of spam and network attacks. Another legal document regulating this area is the Doctrine of Information Security of Ukraine, in which one of the key issues is the provision of technogenic security, including in the field of its information aspects and the fight against technological terrorism. However, it is not an effective regulator in its field. In addition, the law on the principles of state information policy has not been passed. Similarly, a cyber command has not been created in Ukraine, which could quickly respond to challenges in the state security information security.

3. CONCLUSIONS AND PERSPECTIVES FOR FURTHER STUDIES

Analyzing all the above, it can be concluded that within the framework of the EU, information security is considered, first of all, as a state of information networks and systems that provides an adequate level of protection of the integrity, availability, authenticity and confidentiality of information and the appropriate level of counteraction to external negative influences. Priorities of EU policy in the field of information security are the creation and implementation of programs and various technical means of protection of information and communication technologies; development of normative legal acts that establish a list of crimes in the IT sphere and criminal liability; ensuring a high level of public awareness of the risks, threats and ways of protecting their information systems / networks from undesirable effects.

REFERENCES

1. *Німецька кіберзлочинність.* URL: http://www.dw.com/uk/%D1%838C/a-38555191.

2. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security

and resilience. *COM (2009)149.* URL: http://ec.europa.eu/information_ society/policy/nis/strategy/ activities/ciip/index_en.htm.

3. *Кіберзлочинність Франції.* URL: http://www.dw.com/ukB8/a-37057663.

4. *Кібербезпека.* URL: http://start. karazin.ua/programs/5/7/125/31.

5. *Кібератаки проти Естонії.* URL: https://uk.wikipedia.org/wiki97_(2007).

6. *WannaCry.* URL: https://uk.wikipedia.org/wiki/WannaCry.

7. *Збитки WannaCry.* URL: https://www.epravda.com.ua/news/2017/05/25/625286/.

8. *Новий час*. URL: https://nv.ua/ukr/techno/it-industry/eksperti-vijavili-virus-jakij-fizichno-poshkodz huje-smartfoni-dobuvajuchi-kriptovaljuta-2409883.html.

9. Perkins, J. *Policy. Information Security Policy*. London: School of Economics & Political Science IMT, 2018, 24 p.

10. *Комплексний підхід до боротьби з кіберзлочинністю в Європі*. URL: http://dspace. oduvs.edu.ua/bitstream/ 20.pdf.

11. Отчет по информационной безопасности. *Полугодовой отчет Cisco за 2014 год.* URL: https://tucha.ua/wp-content/uploads/cisco_2014_midyear_security_report.pdf.

12. *Global Cybersecurity Index (GCI) 2017*. URL: https://www.itu.int/dms_pub/itu-d/opb/str/ D-STR-GCI.01-2017.pdf.

13. EU Cybersecurity Dashboard. URL: http://cybersecurity.bsa.org/countries.html.

14. *About NorCERT, the Norwegian National Cyber Security Centre.* URL: https://nsm.stat.no/ norcert/norcert-eng/.

15. *The European Network and Information Security Agency.* URL: http://www.enisa.europa.eu/.

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК СУЧАСНА ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЄВРОПЕЙСЬКИХ КРАЇН

Зазначаємо, що ефективна та активна боротьба європейських країн з інформаційним тероризмом відбувається в рамках Європейського Союзу, усіма його країнами-членами, а також державами-сусідами й претендентами на вступ. Тому потрібно наголосити, що Європейський Союз проводить дуже активну політику в галузі інформаційної безпеки. На цей момент він об'єднує високорозвинені країни, які мають величезний вплив на міжнародні відносини, установлюючи норми та стандарти поведінки держав у політичній, економічній, соціальній, інформаційній й інших сферах. Основна мета ЄС – посилити діалог Європейської комісії з міжнародними організаціями та партнерами з питань безпеки мережі й, зокрема, зростаючої залежності від електронних мереж. Політичні пріоритети в галузі інформаційної безпеки, визначені керівними органами Європейського Союзу, реалізуються на національному рівні як державними органами, так і неурядовими організаціями.

Аналізуючи все вищесказане, можемо зробити висновок, що в рамках ЄС інформаційну безпеку розглядаємо, насамперед, як стан інформаційних мереж і систем, що забезпечує належний рівень захисту цілісності, доступності, достовірності та конфіденційності інформації й відповідного рівня протидії зовнішнім негативним впливам. Пріоритетами політики ЄС у сфері інформаційної безпеки є створення та реалізація програм і різних технічних засобів захисту інформаційно-комунікаційних технологій; розробка нормативно-правових актів, що встановлюють перелік злочинів у сфері ІТ та кримінальної відповідальності; забезпечення високого рівня обізнаності населення про ризики, загрози й способи захисту їхніх інформаційних систем / мереж від небажаних наслідків.

Ключові слова: європейські держави, Європейський Союз, кібербезпека, кіберзлочинність, інформаційний тероризм, інформаційна безпека, ENISA.

Матеріал надійшов до редакції 15.11.2018 р.