OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 11, Nº. 1 (May-October 2020), pp. 18-29

JANUS.NET
e-journal of International Relations

COMBATING CYBERCRIME AS A PREREQUISITE FOR THE DEVELOPMENT OF THE DIGITAL SOCIETY

Olga A. Klymenko
ms-kl18@ukr.net
Ph.D. in Law. Head of the Department at the Interagency Research Center on Problems of Combating Organized Crime under the National Security and Defense Council of Ukraine (from 2017 to 2019), Kyiv (Ukraine).

Mykhaylo V. Gutsalyuk
mvgutsalyuk@ukr.net
Ph.D. in Law, Associate Professor. Chief Researcher at the Interagency Research Center on Problems of Combating Organized Crime under the National Security and Defense Council of Ukraine, Kyiv (Ukraine).

Andrii V. Savchenko
savchenkoav@ukr.net
Doctor of Law (LLD). Professor of the Criminal Law Department of the National Academy of Internal Affairs, Kyiv (Ukraine).
.

Abstract

The article deals with the issues of cyber security and cybercrime in the digital society. The areas for improving international cooperation to ensure the security of the Internet are proposed.

Digitized society is being implemented around the world at a high rate and offers significant benefits for the development of both society as a whole and its individual components. At the same time, a factor that has a negative impact on this development is cybercrime. The article explores the current state and main trends of cybercrime, including its organized forms.

The legislative and organizational measures are proposed to counter cybercrime, the leading role of international cooperation is emphasized, including the rapid exchange of electronic data to detect and investigate cybercrime.

Keywords

Cybercrime, Cyber security, International cooperation, Digital society, Counteraction

How to cite this article

Klymenko, Olga A.; Gutsaliuk, Mykhailo V.; Savchenko, Andrii V. (2020). "Combating cybercrime as a prerequisite for the development of the digital society". *JANUS.NET e-journal of International Relations*, Vol. 11, N.º 1, May-October 2020. Consulted [online] on the date of the last visit, https://doi.org/10.26619/1647-7251.11.1.2

Article received on November 12, 2019 and accepted for publication on March 26, 2020

COMBATING CYBERCRIME AS A PREREQUISITE FOR THE DEVELOPMENT OF THE DIGITAL SOCIETY

Olga A. Klymenko
Mykhaylo V. Gutsalyuk
Andrii V. Savchenko

Problem statement

One of the signs of the modern digital society is the rapid development of information technologies and the spread of the Internet, which are being introduced into all spheres of life. The first website in history was created in 1991, and today there are more than 1.8 billion websites in the world. If in 2015 the number of Internet users was about 2 billion, then in 2019 they already exceeded 4 billion (Internet live stats, 2019).

The first-ever Digital Europe programme, proposed in June 2018, will invest in five key digital sectors: high performance computers, artificial intelligence, cybersecurity and trust, advanced digital skills, and ensuring the wide use and deployment of digital technologies across the economy and society, in order to strengthen European industrial technological leadership (EU Budget, 2018).

At the same time, with the development of computer technology, a new form of criminal activity appeared – cybercrime, which today has mastered the environment of computer networks and mobile devices. The anonymity of global information networks, the speed of information transfer makes it possible to use these advantages not only for the development of the information society, but also for the commission of unlawful acts. This is also facilitated by the fact that information and communication technologies are being introduced and are developing much faster than legislators and law enforcement agencies can react to. Therefore, the sustainable development of a digital society is only possible if the cybercrime is actively combated, including its organized forms.

Cybercrime, unlike the traditional ones, is characterized by the fact that they are committed using computers and data networks, including the global Internet. As a result, such crimes can be transboundary in nature and perpetrated by organized criminal interstate groups. Another feature is that the evidence of such crimes is contained in electronic devices (electronic or digital evidence) and has the ability to be quickly modified or even destroyed.

After the World Health Organization recognized the coronavirus as a pandemic, many organizations around the world began to introduce remote methods of work in their units, including organizations such as the US Congress, the Pentagon, NASA. At the same time, Internet traffic has increased significantly. For example, Webex web conferencing traffic has grown 22 times! (Free video conferencing: Coronavirus spurs special deals from

WebEx, Google, others, 2020). In such conditions, the reliability of telecommunications increases significantly.

The corporate culture will not be the same after coronavirus. Some of the companies will remain distant after the global epidemic. Firstly, the employees themselves, having felt the benefits of homework, will not want to return to offices. And secondly, business owners, having measured the KPI of employees and savings on rental premises and utilities, can leave only the most necessary employees in the office.

Cybercrime and cybersecurity measures

If cybercrime in the last century were relatively rare events and investigated within individual states, at the beginning of XXI century, they have become one of the most pressing problems that confronted the international community and began to actively seek mechanisms for combating this phenomenon (Eoghan Casey, 2011, Marie-Helen Maras, 2016), in particular:

- in 2001, the Convention on Cybercrime was adopted in Budapest. This document sets out a list of cybercrimes and the procedural provisions necessary to combat cybercrime, including the collection and sharing of electronic evidence (Convention on Cybercrime 2001);
- in 2002, the First International Strategic Congress on Cybercrime "E-Crime Congress 2002" devoted to the problems of fighting electronic crimes was held in London. At the congress, the representatives of law enforcement agencies of different countries and IT industry discussed issues of effective counteraction to cybercrime (Gutsalyuk M. V. Fighting Cybercrimes, 2002);
- in 2004, in accordance with Regulation (EU) No 460/2004, the European Network and Information Security Agency (ENISA) was established, whose main task was to improve network and information security in the European Union (Regulation (EC) No 460/2004);
- in 2007, the International Telecommunication Union (ITU) developed the Global Cybersecurity Program (GCA) as a framework for international cooperation aimed at enhancing confidence and security in the information society (Global Cybersecurity Agenda, 2007);
- in 2010, at the UN a group of experts was created to conduct cybercrime research. The group prepared a comprehensive study of cybercrime (Comprehensive Draft Study on Cybercrime, 2013);
- in 2011, the International Strategy for Cyberspace was developed in the USA (International Strategy for Cyberspace, 2011);
- in 2013, the EU Directive on cyberattacks on information systems was adopted (Directive 2013/40/EU);
- in 2013, in accordance with Regulation (EU) No 526/2013, the European Union Agency for Network and Information Security was established and Regulation (EU) No 460/2004 was repealed (Regulation (EU) No 526/2013);
- in 2013, Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect

European citizens, businesses and governments from online crime (European Cybercrime Centre, 2013);

- in 2014, the National Institute of Standards and Technology developed a Critical Infrastructure Framework for Critical Infrastructure Facilities to detect, prevent and respond to cyberattacks (Framework for Improving Critical Infrastructure Cybersecurity, 2014). In April 2018, a new version 1.1 of this document was released;
- in 2016, EU Directive 2016/1148 on measures to ensure a high overall level of safety of network and information systems throughout the Union was adopted (Directive (EU) 2016/1148, 2016);
- in 2017, European Commission President Jean-Claude Juncker announced a Cyber Security package setting out measures of responding to the change cyber-threats landscape (Cyber Security Package, 2017);
- in 2018, the General Data Protection Regulation (GDPR), the European Union directive on the use of personal data, has come into force (General Data Protection Regulation, 2018);
- in 2019, Europol announced the adoption of a new protocol for how law enforcement authorities in the European Union and beyond will respond to major cross-border cyberattacks. The new protocol, adopted by the Council of the EU, is part of the EU's Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises, and it will be implemented by Europol's European Cybercrime Centre (EC3) (EU Adopts New Response Protocol for Major Cyberattacks, 2019).

It should be noted that in recent years all developed countries have also adopted relevant national legislation on the criminal prosecution of cybercrime, developed strategies to combat them and created the appropriate law enforcement units (Gutsalyuk, 2016).

The current state of affairs and the latest cyber security challenges

However, cybercrime continues to spread and grow. According to survey of PWC (PricewaterhouseCoopers), cybercrime was more than twice as likely than any other fraud to be identified as the most disruptive and serious economic crime expected to impact organizations in the next two years (PwC's Global Economic Crime and Fraud Survey, 2018).

Experts of the World Economic Forum in Davos in January 2018 published an annual report on global risks in the world, entitled "Global Risks Report 2018" (Global Risks Report, 2018). Based on its concepts, cyberattacks are in the second place in terms of negative influence for the world community after extreme weather events (i.g., a year ago technological risks along with cybercrime occupied the third place). The report states that the risks of cyber security are constantly increasing. For example, cyberattacks on businesses have doubled in the past five years, and incidents that were once considered extreme have become more common today, and hackers attack computers and networks at "almost constant speed" – every 39 seconds there is one cyberattack (Milkovich Devon, 2019).

Lloyd's of London said in a report that major, global cyberattack could trigger an average of $53 billion of economic losses, including losses from the WannaCry attack in May 2017, which affected 300,000 computers in 150 countries, amounting to $850 million and from attacks on another computer virus that spread in Ukraine in June 2017 amounted to $850 million (Gutsalyuk, Klymenko, 2017; Global cyberattack could spur $53 billion in losses, 2017).

According to the 2018 Cyber Incident Statistics (ENISA) malicious activity and system crashes are the dominant cause of reported incidents: system crashes make up 39% of the total cases (36% in 2017, respectively). Malware rose to 39% (up from 7% in 2017) (Annual report Trust Services Security Incidents, 2018).

In the modern era of strategic competition, cyber espionage is taking a new leap. The UK's Government Code and Cipher School (GCCS) estimates that there are 34 separate nations that have serious well-funded cyber espionage teams. These state-based threat actor teams are comprised of computer programmers, engineers, and scientists that form military and intelligence agency hacking clusters. They have tremendous financial backing and unlimited technological resources that help them evolve their techniques rapidly (Cyber Espionage Is Global – and Taking Warfare to a New Level, 2018).

One of the latest technological tools for cyberattacks, which are currently actively developing, is the use of Machine Learning and Artificial intelligence – AI. Since it is becoming easier to create viruses and carry out large-scale attacks over time, around organized cybercrime today there is a massive cybernetic subculture, and in the coming years, the level of cybercrime and the active self-organization of hackers are expected to increase.

In addition, more and more countries are implementing cyberforces that can influence the infrastructure of the "opponents". According to the UN Secretary-General, Antonio Guterres, during a speech at the University of Lisbon on February 19, 2018: "The next war will begin with a mass cyberattack aimed to destroy military capabilities and to paralyze basic infrastructure such as electrical grids". Guterres called for the unification of the world community in order to minimize the influence of cyber wars on the lives of civilians and suggested creating a platform in the United Nations on the basis of which scientists, officials and others could develop rules "to ensure a more human nature" in resolving any conflict related to information technologies (Khalip Andrei, 2018).

One of the current trends in information technology is the large-scale introduction in most countries of cryptocurrencies, which become a complete payment instrument and investment asset. The total market capitalization of the cryptocurrencies in 2017 exceeded $500 billion US dollars. However, it should be noted that Bitcoin and other digital currencies are adapted for use by organized criminal groups, since they are widely used in international circulation and provide the necessary level of anonymity. For example, in 2017, during the kidnapping of people in Kyiv, Vinnitsa, Odessa (Ukraine), cybercriminals demanded a ransom in a crypto currency in the amount of several million US dollars (Of the 507 abductions in 4 cases, the perpetrators demanded a ransom in bitcoins, – National Police, 2018).

Because of the high cost of the cryptocurrency, it attracts the intruders. In January 2018, one of the largest digital exchanges in Japan, Coincheck, reported a loss of about $534 million in cryptocurrency due to a hacker attack on its network. The Exchange will

reimburse 260,000 customers at its own expense (Coincheck promises 46bn yen refund after cryptocurrency theft, 2018).

It is also becoming common the term "cryptojacking" – the secret use of computers for mining the crypto currency. The research team at Palo Alto Networks 42 has revealed a large-scale operation on mining Monero, which has been active for 4 months. The number of victims affected by this operation is approximately 15 million people worldwide (Grunzweig Josh, 2018).

Given the fact that the extent of cybercrime is constantly increasing, Interpol, in February 2017, has developed a Global Strategy to Combat Cybercrime. The document states that law enforcement agencies face problems related to a cross-border investigation, a variety of legislation and technological opportunities around the world. The program to combat cybercrime is coordinated by Interpol through the Global Complex for Innovation in Singapore, which is equipped with a digital forensics laboratory and an innovation center that provides Interpol with the ability to provide a consistent and effective approach to combating all forms of transnational crime.

The report of the European Cybercrime Centre (EC3) – "Internet Organized Crime Threat Assessment" – IOCTA evaluated key events, changes and threats in the field of cybercrime in 2019, and made the following key findings:

- ransomware remains the top threat. Attackers focus on fewer but more profitable targets and greater economic damage;
- data remains a key target, commodity and enabler for cybercrime;
- following the increase of destructive ransomware, such as the Germanwiper attacks of 2019, there is a growing concern within organisations over attacks of sabotage;
- continuous efforts are needed to further synergise the network and information security sector and the cyber law enforcement authorities to improve the overall cyber resilience and cybersecurity;
- the dark web remains the key online enabler for trade in an extensive range of criminal products and services and a priority threat for law enforcement;
- terrorist groups are often early adopters of new technologies, exploiting emerging platforms for their online communication and distribution strategies.

The report of the European Cybercrime Centre provides the following recommendations for counteracting organized cybercrime: a) law enforcement agencies should continue to focus on the actors that develop and provide tools and services for cyberattacks; b) law enforcement and the private sector should continue to work together to analyze threats and initiatives such as the project "No More Ransom" to raise awareness and provide advice and free tools for deciphering cyberattack data; c) today's ransomware developers are increasingly relying on social engineering. Training of employees of organizations on counteraction to attempts of social engineering will prevent many cyberattacks. Today, the probability of personal data thefts has increased significantly (while hacking the information system of one of the corporations, the attackers seized personal information of 147 million people) (Equifax to Pay $575m in Data Breach Settlement, 2019). More than a million fingerprints and other sensitive data have been exposed online by a biometric security firm, researchers say (Baraniuk Chris, 2019).

Future threats and challenges

In general, we can state that at the present the number of cybercrimes directed to mobile platforms is growing most dynamically, in which the number of ransomware detections has doubled in recent years. Dangerous in the expert environment is also considered the dynamic development of the Internet of things (IoT), with the use of which it is projected an increase of the number of cyberattacks.

In this regard Japan has approved a law amendment which allows government officials to hack into people's Internet of Things (IoT) devices. The amendment is part of a survey investigating the number of vulnerable IoT devices carried out by the National Institute of Information and Communications Technology (NICT) under the supervision of the Ministry of Internal Affairs and Communications (MIC). Japan is carrying out the survey to prevent the devices from being harnessed for a cyberattack targeting infrastructure supporting the Tokyo Olympic Games in 2020. NICT employees will have permission to attempt the hacking of IoT devices using default passwords and password dictionaries. Users leaving passwords set as their device manufacturer's default is often how devices are compromised. Japan's approach is an unprecedented but proactive way of dealing with the IoT security problem. A report published by the MIC highlighted two-thirds of cyberattacks in 2016 were targeted at IoT devices (Daws Ryan, 2019).

Among the factors that hinder the counteraction of organized crime in cyberspace, remain the following: a) transnational nature of offenses, which consists in the fact that the place of commission, the instrument of crime, the victims and the offender may be under different territorial jurisdictions and there is a need for many formal interstate agreements to investigate such crimes, which significantly slows down their conduct; b) high level of technical training of criminals; c) problems of collecting electronic (digital) evidence that can be rapidly changed or even destroyed; d) the difficulty of identifying offenders – since the individual "signatures" of offenders is leveled by a standardized instrument of commission – by software and technological support; e) lack of sufficient judicial practice in criminal cases on organized crime in the field of information technology.

Due to the fact that computer data can be easily altered or even destroyed, Articles 16–21 of the Cybercrime Convention 2001 provide for the application of legislative and other measures for the urgent storage of computer data, data traffic, interception and real-time information recording time scale to be implemented by all signatory states. It is advisable to exchange such information through the relevant 24/7 points created in all countries. However, due to various circumstances, responses to requests for such information may be delayed for a long time, rendering such information out of date and preventing cybercrime investigation. Therefore, international cooperation in this area needs improvement.

For proper investigation of cybercrimes, it is important to organize close cooperation of law enforcement agencies with service providers (Internet providers) for rapid disclosure of data, and to improve mutual legal assistance procedures that relate to electronic data in order to promptly obtain electronic evidence. At the same time, law enforcement agencies already have a significant positive experience of intergovernmental cooperation in combating cybercrime.

A striking example of this was the operation to eliminate the cyber network "Avalanche", which functioned for about 7 years and infected thousands of computers daily, and the financial losses from attacks amount to more than 100 million Euros. The investigation was conducted by the Verdun Prosecutor's Office and the police in Lüneburg (Germany) in close cooperation with the Ministry of Justice and the FBI, Eurojust, Europol and global partners. 178 people were arrested by law enforcers with the support of the European Cybercrime Center (EC3) and the Joint Cybercrime Action Taskforce (J-CAT) as well as Eurojust and the European Banking Federation (EBF). On the territory of Europe, 580 so called "drones" (persons involved in cashing in of money) were identified. A successful attack on this international organized criminal group was supported by 106 banks and private partners. More than 130 TB of collected data were analyzed at the stage of preparation of a special operation by cyberpolice. During the joint operation, conducted on the 30th of November 2016 in 30 countries, five network organizers were detained. Three of them are Ukrainians; one was detained in Germany, two more – on the territory of Ukraine. One of the organizers of the criminal group is charged with 1152 crimes, which caused a loss of 6 million Euros ('Avalanche' network dismantled in international cyber operation, 2016).

And in February 2018, the US Department of Justice filed a charge of cyber-scam about 36 people suspected of participating in the international groupings of the Infraud Organization, created by a citizen of Ukraine. It is noted that the group stole more than $530 million. Organization illegally received and sold personal data of network users, was engaged in hacking of banking and electronic accounts, and also distributed malicious software. According to US law enforcement officers, about 11,000 people were involved in the Infraud Organization, most of whom never met personally (Thirty-six Defendants Indicted…, 2018).

With the growing popularity of the Internet, and given that e-commerce is becoming the most important part of the economy with turnover, measured by trillions of US dollars (Retail e-commerce sales worldwide from 2014 to 2021, 2019), the number of cybercrime will increase accordingly. Therefore, there is a need to create and use national, and ideally even international, means of information analysis. Moreover, cybercrimes require an analysis for a shorter period than days, weeks, or even months, which tend to be based on the analysis of traditional crimes. At the same time, it should be noted that human rights organizations argue that massive amounts of accumulated information do not allow systematically prevent cybercrime, and instead, mass storage of personal data opens up wide opportunities for various kinds of abuse. Given this, on May 2014 decision by the European Court of Justice (ECJ) declared that the European Data Retention Directive was a gross violation of privacy rights under European law and, therefore, was invalid (Judgment of the Court of Justice of the European Union, 2014).

Finally, in addition to combating cybercrime, a necessary element of the safe and efficient functioning of a digital society is the reliable identification of its participants. As we know, all criminals are trying to hide their identity, so in contrast to Darknet, whose main feature is anonymity, you need to create electronic services that only work with verified users. Electronic digital signatures, or other mechanisms, such as electronic ID documents, are likely to be used for verification to ensure that both the user of the service and the Internet resource are verified. This in turn will significantly reduce the number of cyber frauds and other offenses in cyberspace.

Conclusions

In our opinion, among the issues of effective counteraction to cybercrime are still relevant today the following:

1. Development rules of law for conducting searches of electronic evidence, taking into account the possibility of finding it in different jurisdictions (Khakhanovskyi, Hutsaliuk, 2019).
2. Development of specialized software and hardware for the collection, storage and analysis of electronic evidence, including large computer evidence cases.
3. Improvement of the network of National Contact Points for Responding to Cybercrime (24/7) and existing International Legal Assistance mechanisms.
4. Organization of close cooperation between law enforcement agencies and providers for obtaining electronic evidence.
5. Regular rising of qualifications of investigators and other involved law enforcement officers in order to study topical issues of the tactics of conducting investigative actions to obtain electronic evidence in the cybercrime investigation.
6. In order to increase the effectiveness of cybercrime investigations, specialized structural units should be established in both the police and prosecutors' offices, and possibly specialized courts.
7. Increasing the level of cyber security in both public and private sectors, as well as developing new technologies for protecting and identifying users of cyberspace. The Global Cybersecurity Center, created in Geneva under the auspices of the World Economic Forum, should assist in close collaboration of business, academics and government officials on cyber security.

Only through cooperation of all stakeholders, information exchange and common standards, the world community will be able to successfully counter cybercrime. The fulfillment of these measures will allow obtaining in full the advantages of the digital society.

References

'Avalanche' network dismantled in international cyber operation (The Hague, 01 December 2016). [Accessed on 16 September 2019]. Available at: http://www.eurojust.europa.eu/press/PressReleases/Pages/2016/2016-12-01.aspx.

Annual report Trust Services Security Incidents 2018 [Accessed on 8 September 2019]. Available at: https://www.enisa.europa.eu/news/enisa-news/annual-report-trust-services-security-incidents-2018.

Baraniuk Chris. Biostar security software 'leaked a million fingerprints' (August 14, 2019) [Accessed on 15 September 2019]. Available at: https://www.bbc.com/news/technology-49343774.

Coincheck promises 46bn yen refund after cryptocurrency theft (January 28, 2018) [Accessed on 10 September 2019]. Available at: http://www.bbc.com/news/world-asia-42850194.

Comprehensive Draft Study on Cybercrime (Draft – February 2013) [Accessed on 26 August 2019]. Available at: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.

Convention on Cybercrime 2001 [Accessed on 23 August 2019]. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Cyber Espionage Is Global – and Taking Warfare to a New Level (2018). [Accessed on 9 September 2019]. Available at: https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/.

Cyber Security Package (2017) [Accessed on 3 September 2019]. Available at: https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/cyber-security-package/Pages/default.aspx.

Daws Ryan. Japan's law now allows it to hack people's IoT devices (January 29, 2019). [Accessed on 15 September 2019]. Available at: https://www.iottechnews.com/news/2019/jan/29/japan-law-hack-iot-devices/.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016) [Accessed on 2 September 2019]. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [Accessed on 28 August 2019]. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040.

Eoghan Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 2011. P. 840.

Equifax to Pay $575m in Data Breach Settlement (July 22, 2019) [Accessed on 12 September 2019]. Available at: https://www.phishprotection.com/watchdog/.

EU Adopts New Response Protocol for Major Cyberattacks (2019) [Accessed on 5 September 2019]. Available at: https://www.securityweek.com/eu-adopts-new-response-protocol-major-cyberattacks.

EU budget: Commission proposes € 9.2 billion investment in first ever digital programme (Brussels, 6 June 2018). [Accessed on 23 August 2019]. Available at: https://europa.eu/rapid/press-release_IP-18-4043_en.htm.

European Cybercrime Centre (2013) [Accessed on 1 September 2019]. Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Framework for Improving Critical Infrastructure Cybersecurity (2014) [Accessed on 2 September 2019]. Available at: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11.

Free video conferencing: Coronavirus spurs special deals from WebEx, Google, others URL: [Accessed on 30 March 2020] Available at: https://www.zdnet.com/article/video-conferencing-deals-coronavirus-spurs-offers-from-webex-google-and-others/.

General Data Protection Regulation (2018) [Accessed on 3 September 2019]. Available at: https://gdpr-info.eu/.

Global cyberattack could spur $53 billion in losses: Lloyd's of London (2017) [Accessed on 8 September 2019]. Available at: https://www.cnbc.com/2017/07/17/global-cyberattack-could-spur-53-billion-in-losses-lloyds-of-london.html.

Global Cybersecurity Agenda (GCA) (2007) [Accessed on 26 August 2019]. Available at: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

Global Risks Report 2018 [Accessed on 7 September 2019]. Available at: https://www.weforum.org/reports/the-global-risks-report-2018.

Grunzweig Josh. Large Scale Monero Cryptocurrency Mining Operation using XMRig (January 24, 2018) [Accessed on 12 September 2019]. Available at: https://unit42.paloaltonetworks.com/unit42-large-scale-monero-cryptocurrency-mining-operation-using-xmrig.

Gutsalyuk Mykhaylo, Klymenko Olga. Combate á criminalidade cibernética e garantias de segurança cibernética na Ucrânia // Lusiada. Política Internacional e Segurança, 2017, nª15. P. 51–65. [online] Available at: http://revistas.lis.ulusiada.pt/index.php/lpis/article/view/2506/pdf [Accessed 2 March 2018].

Gutsalyuk Mykhaylo. Ukraine's Cybersecurity Strategy and Ways to Implement It // European Cybersecurity Journal. – Volume 2 (2016). The Kosciuszko Institute. Poland. – P. 65–69. [Accessed on 6 September 2019]. Available at: https://twitter.com/i/moments/781827366100140032.

Gutsalyuk M. V. Fighting Cybercrimes (2002) [Accessed on 24 August 2019]. Available at: http://www.crime-research.org/library/Gutsaluk.html.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0460.

International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World (May 2011) [Accessed on 28 August 2019]. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Internet live stats (2019) [Accessed on 23 August 2019]. Available at: http://www.internetlivestats.com.

Internet Organized Crime Threat Assessment (IOCTA) (2019) [Accessed on 11 October 2019]. Available at: https://www.europol.europa.eu/iocta-report.

Judgment of the Court of Justice of the European Union (Date of decision/judgment: 13/05/2014) / ECLI:EU:C:2014:317. [Accessed on 17 September 2019]. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

Khakhanovskyi Valerii, Hutsaliuk Mykhaylo. The Peculiarities of Digital Evidence Use in Criminal Proceedings // Kryminalistychnyi Visnyk, Vol 31, No 1 (2019). pp. 13–19. DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13.

Khalip Andrei. U.N. chief urges global rules for cyber warfare (February 19, 2018) [Accessed on 8 September 2019]. Available at: https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.

Marie-Helen Maras. Cybercriminology. Oxford University Press, 2016. P. 448.

Milkovich Devon. 15 Alarming Cyber Security Facts and Stats (September 23, 2019) [Accessed on 25 September 2019]. https://www.cybintsolutions.com/cyber-security-facts-stats/.

Of the 507 abductions in 4 cases, the perpetrators demanded a ransom in bitcoins, – National Police (January 26, 2018) [Accessed on 10 September 2019]. Available at: https://112.ua/obshchestvo/iz-507-pohishheniy-v-4-sluchayah-zloumyshlenniki-trebovali-vykup-v-bitkoinah-nacpoliciya-430498.html.

PwC's Global Economic Crime and Fraud Survey 2018 [Accessed on 6 September 2019]. Available at: https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html.

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) [Accessed on 25 August 2019]. Available at:

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance) [Accessed on 1 September 2019]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0526.

Retail e-commerce sales worldwide from 2014 to 2021 (in billion U.S. dollars) / By J. Clement, last edited Aug 30, 2019 [Accessed on 17 September 2019]. Available at: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes (Wednesday, February 7, 2018) / Department of Justice / Office of Public Affairs. [Accessed on 16 September 2019]. Available at: https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible.