Criminological Features of the Cybersecurity Threats

Submitted: 6 December 2022
Revised: 29 January 2023
Reviewed: 10 March 2023
Accepted: 15 March 2023

Viktor Anatolievich Shestak[*]
https://orcid.org/0000-0003-0903-8577
Alyona Dmitrievna Tsyplakova[**]
https://orcid.org/0000-0001-8564-0696

Article submitted to blind peer review

DOI: https://doi.org/10.26512/lstr.v15i2.45997

Abstract

[Purpose] Currently, novel tools have converted many traditional phenomena into cyber ones. The absence of a standardized terminology and classification of cybersecurity threats has raised significant concerns among researchers and lawmakers. Ignoring the emerging risks that necessitate appropriate responses is impracticable. Prior to devising countermeasures to combat cybercrime, it is imperative to accurately define the concept of cybersecurity threat and differentiate it from other related notions such as information security, computer security, cyberattack, cyberspace attack, cyber incident, cybersecurity incident, cyber threat, and cybersecurity event, whose definitions may be ascertained from the glossaries of various standardization institutes.

[Methodology/Approach/Design] This study presents a descriptive investigation of cybersecurity threats and their causes, utilizing genetic, systematic-functional, and systematization methods. Cyberattacks are identified as the primary threat, and data is represented through qualitative research and summarized in tables. The study also considers the historical background of concepts and cyber-criminality.

[Findings] The present study delves into a comprehensive analysis of distinct categories of cybersecurity threats, the trajectory of cybercrime, and the factors that underpin the emergence of new cybersecurity threats. The research scrutinizes both the general causes for cyber-criminality and the specific determinants for criminal activities that target the energy sector, a critical component of a state's infrastructure. The study reveals that the major sources of threats comprise terrorists, insiders (i.e., disgruntled employees), commercial spies, and black hackers or crackers, whose malicious acts are themselves considered threats to cybersecurity.

[*]Doctor of Juridical Science, Professor of the Department Criminal Procedure, Moscow Academy of the Investigative Committee of the Russian Federation (Moscow, Russian Federation). Address: 12, Vrubel Street, Moscow, Russia, 125080. E-mail: viktor_shestak@mail.ru.
[**]Bachelor of Laws (LL.B.), Master's Degree Student of the Department of Criminal Law, Criminal Procedure and Criminology of MGIMO University (Moscow, Russian Federation). E-mail: tsyplakova.a.d@my.mgimo.ru.

Keywords: Cybersecurity Threats. Criminology. Information Security. Cybersecurity. Determinants of Crime.

INTRODUCTION

Undoubtedly, it is the regulation of information and telecommunication technologies that arouses a lot of scientific interest. According to McKinsey Global Institute, more than half of operations will be automated in the next 20 years(Ovchinsky V. S., 2016: 9). According to Kaspersky Lab., the share of cyber aggression accounts for 49,48% (Kaspersky Lab., 2020). As to the short-term and medium-term risks, half of respondents rank cybersecurity as one of the top challenges, according to the World Economic Forum (World Economic Forum, 2021). Despite the fact that in the early 2000s fight against cyber threats was not considered primary, statistics show that most frequently committed crimes are cyberattacks, which can be committed within a company, a state and outside it. For instance, in the USA in September 2021, it was recorded that over the summer 77% of all companies in the fuel and energy sector were subject to employee data leakage. In 2020, the most popular scheme was DDoS attacks, and in 2021 it was phishing (in 65% of cases) (Nescout, 2021).

REVIEW OF KEY NOTIONS

Researchers have been elaborating the notion hierarchy, but it is treated as tentative. One may define information security (InfoSec) as the state of being secured vis-a-vis any information, regardless of its form of expression and medium. It is based on a triad of principles: integrity, availability and confidentiality. Cybersecurity is only an element of InfoSec and concerns the digital assets, including data in cyberspace and on any e-device. Due to the complexity of the digital world, the hardship arises with computer security that implies the use of such a specific device as computer, but it considers a narrow approach to the phenomenon in question.

Taking into account to the International Organization for Standardization, it is worth reviewing the standard ISO/IEC 27001: 2013 “Information technology — Security techniques — Information security management systems”. Cybersecurity is defined as actions and security controlling methods used to protect against cyberattacks. National Institute of Standards and Technology (NIST) Glossary provides broader interpretations of cybersecurity:

(1) Prevention of damage to, protection of and restoration of computers, electronic communications systems and services, wire and electronic communication, including information contained therein, to ensure its

availability, integrity, authentication, confidentiality and nonrepudiation;
(2) Process of protecting information by preventing, detecting, and responding to attacks;
(3) Ability to protect or defend the cyberspace against cyberattacks;
(4) Prevention of damage to, unauthorized use of, exploitation of the restoration of electronic information and communications systems (ICS) (if needed) and the information contained therein, in order to enhance the confidentiality, integrity and availability of these systems.

Cyberspace is described as the following:

(1) Global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries;
(2) Complex environment which results from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it and does not exist in any physical form.

Nevertheless, one should take into account the fact that cybersecurity threats are far beyond cyberattacks, therefore, in the American researchers and policy makers broadly interpret the term cybersecurity, scrutinizing such notions as cyberattack, cyberspace attack, cyber incident, cybersecurity incident, cyberthreat, cybersecurity event.

A cyberattack is an attack committed via cyberspace and aimed at disrupting, disabling, destroying a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information. Meanwhile, a cyberspace attack has a more general characteristic, i.e., cyberspace actions that create various negative effects and manipulation leading to denial, however, it is insufficient to underline specific features of the phenomenon under consideration.

Actions that constitute a cyber incident are those taken through the use of an information system or network (IS/N) that result in an actual or potentially adverse effect on an IS/N and/or the information stored therein. The definition of the cybersecurity incident empathizes the necessity of response to the impact that actually or inevitably jeopardizes the triad of principles and constitutes a violation or imminent threat of violation of a law, security policy or acceptable use. The clarification of a cybersecurity event undermines consequences that have impact on the organization's activities, its capabilities or reputation. At the

same time, the concept of an incident can include not only deliberate attacks as a threat to obtain unauthorized access and data theft or falsification, but also unintended consequences, such as damage, incorrect operating systems and unauthorized changes to their configurations (Belous A. I., 2020: 229–230).

A cyberthreat is any circumstance, condition or event that may adversely affect the organizational operation, mission, functions, image, reputation, assets, or individuals, or other organizations, or the state, or the Nation through IS/N via unauthorized access, destruction, disclosure, modifications of information and/or denial of service. It is also considered undesirable potential loss.

As it is stated in the Glossary, regardless the specific term used, the basis constitutes all forms of (un)intentional, accidental or incidental, misuse or abuse, error, vulnerabilities, defect, fault and/or failure and their associated conditions. One may conclude that the concepts of cyber threat and cybersecurity threat are corresponding and reflect the features under consideration in full. The most famous cyberattacks on energy sector, military, transportation, entertainment banking and finance sphere are summarized in Table 1 (Desarnaud G., 2017; Livingston S., Sanborn S., Slaughter A., Zonneveld P., 2019; Kovacs E., 2018; Petcu A.G., 2022, Kaspersky E., 2017).

Year	Target	Act	Description and Consequences
1992	Ignalina nuclear-power station, (Lithuania)	Sabotage	Virus in the control system of a RBMK reactor.
1992	Emergency warning system at Chevron (USA)	Sabotage	An employee fired from the company hacked computers in charge of emergency warning system. A crash and explosion of toxic substances occurred at a refinery.
1999	Olympic (gas) pipeline in Bellingham (Washington D.C., USA)	Failure in SCADA (supervisory control and data acquisition system)	Oil spillage, 3 deaths and a number of injuries.
2001	Electricity operator (California, USA)	Sabotage attempt	Having got access to Independent Controlling System, the hackers failed.
2003	Davis-Besse	Cyberattack	Shutdown of the

	Nuclear power plant (Ohio, USA)	(Slammer)	parameter display system for 4 hours.
2008	Edwin I. Hatch nuclear power plant (Georgia, USA)	Human error (?)	Due to incorrect system update, there was an unintentional shutdown for 48 hours.
2008–2012	(Middle East)	Cyberattack (Narilam)	Data theft and small corruptions
2010	Natanz nuclear facilities (Iran)	Cyberattack (Stuxnet) by the Olympic Games	This type of sabotage damaged more than 900 uranium enrichment centrifuges.
2011	Energy industries (Iran, Sudan)	Cyberattack (Duqu)	Its operation relates to Stuxnet worm, but aims at gathering information (espionage) rather than destruction.
2011	Nuclear company Areva (France)	Cyberattack	Theft of non-critical data
2012	Energy companies (mainly, Middle East and North Africa, but also North America and Europe)	Cyberattack (Flame, Flamer, sKyWIper, Skywiper)	Espionage
2012	Saudi Aramco (Saudi Arabia) and RasGas (Qatar)	Cyberattack (Shamoon, W32.DistTrack)	Sabotage overwrote 30,000 hard disks, but had no impact on the operational network.
2012	Middle East	Cyberattack (Groove)	Time bomb
2013	Bowman Avenue Dam (New York, USA)	Cyberattack	Successful attempt to intrude in safety system. No consequences.
2013	Financial, military and media sectors (South Korea)	Cyberattack (Dark Seoul, Operation 1Mission) by Lazarus	32,000 frozen computer terminals terminated operation of 3 TV station, ATMs. Information leak of 200,000 citizens, 22,000 military personnel.
2013–2014	Energy and industrial	Cyberattacks (Energetic Bear)	Successful sabotage, data collection

	companies, aviation, education and healthcare system (USA and Europe)	using vulnerability of Windows and Citrix	(espionage).
2014	Sony (USA)	Cyberattack by Guardians of Peace	Related to Shamoon. Essential information leak.
2014	Korea Hydro and Nuclear Power, (South Korea)	Blackmail	Theft of plans and manuals of two reactors, electricity circuits, measures of radiation exposure in the zone, and data on more than 10,000 employees and 3 reactors closed.
2015–2017	250 energy American and European companies (electricity producers, electricity and oil distribution operators, equipment producers)	Phishing cyberattacks (Dragonfly)	Administrative operation under control, data collection (espionage), credit data theft and successful sabotage.
2016–2017	Government, industry, telecoms and transportation (Saudi Arabia)	Cyberattack (Shamoon 2)	Sabotage of 11 organizations. 35,000 computers collapsed.
2016–2017	Saudi Arabia and other countries of Middle East	Cyberattack (StoneDrill) by APT33 and Elfin	Related to Shamoon 2. Espionage.
2017	Saudi Arabia	Mamba Ransomware	Decryption of hard drives
2017	Petrochemical plants, power stations (Saudi Arabia)	Cyberattack (Trisis, Triton)	Sabotage that disables safety instrumented systems.
2018	Gas, oil and electricity operator (USA)	Cyberattack on cloud services	Stopping computers and ransom payment demand for encrypted files. At least, 5 companies stopped

			pipeline operation. Some big energy delivers had to stop transactions, under receiving or not receiving money due to miscalculated bills.
2018 – 2021	Oil and gas industry (Saudi Arabia, the UAE, India, Scotland and Italy)	Cyberattack (Shamoon 3)	Oil and gas services company Saipem reported that the malware wiped 300–400 servers and up to 100 PCs (4,000 machines).
2019	USA	Cyberattack (Dridex)	Banking trojan helped to steal more than 70 US dollars from victims' bank accounts.
2021	Natanz nuclear facilities (Iran)	Sabotage or cyberattack	A power blackout damaged machine. Authorities suspect cyber terrorism
2021	Colonial Pipeline (Texas, USA)	Cyberattack (data encryption) by Anonymous Group	13 states introduced emergency regime, 45% transit of East Coast was blocked for 6 days. A ransom in 75 bitcoins was paid (FBI succeeded in tracing and returning 66 bitcoins).

Table 1 – Most Commonly Known Cyberattacks Around the World.

National Cyber Threat Assessment from Canadian Centre for Cyber Security provides a shorter version with an intriguing ambiguity. A cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity or confidentiality of a system or the information it contains[1]. The security of an information system resembles of information security that protects data in general, while cybersecurity involves

[1] Canadian Centre for Cyber Security. *National Cyber Threat Assessment. An Introduction to the Cyber Threat Environment.* Available at: https://cyber.gc.ca/sites/default/files/cyber/publications/Intro-ncta-2020_e.pdf.

network, application, operational, cloud and IoT securities, which implies the processes and technologies as well (IT governance).

RESULTS AND DISCUSSION

Classification

The scholars note the lack of uniform terminology and unified classification of cybersecurity threats. The latter includes the activities of hackers (including hacktivists, botnet operators, phishers, spammers, authors of spyware and/or malware), insiders (commercial spies and disgruntled employees), cyber-terrorists, cyber-extremists, individual organized crime groups and even foreign intelligence services, as well as man-made disasters (See Table 2).

Type	Characteristics
Botnet	Hackers operating some systems to coordinate attacks and dissimilate phishing, spam and malwares
Organized Criminal Groups	Attacks often aim at monetary gain via spam, phishing, spy- or malware to steal personal data and e-fraud
Foreign Intelligence Service	One of the goals is information warfare and critical infrastructure decommission
Hackers (Including Hacktivists)	Applying malware or other instruments in order to cause failure and serious damage
Insiders	Disgruntled employees of an organization who do not obviously have specific knowledge in IT, but have access to ESM. The motive is often revenge which harms not only company's reputation, but critical infrastructure facilities
Phishing	Persons or small groups that steal personal data or information in general in order to take advantage via spam and spy- and/or malware software
Spammers	Persons or organizations that send e-mails with hidden or false information in order to sell produce, activate phishing, spy- or malware software and attacks on organization
The Authors of Spy- and/or Malware Software	Persons or organizations that create or dissimilate spy- or/and malware software, computer virus and worms which damage files and hard drives
Cyber-Terrorism and Cyber-Extremism	Persons or organizations that seek to destroy, disable or use critical infrastructure to compromise national security, weaken a nation's economy and use phishing schemes or spy- and/or malware to obtain funds or gather sensitive

	information
Commercial Spies	More professional approach rather than insiders and the motivation is private gain

Table 2 – Most Commonly Known Cyberattacks Around the World.

In the beginning, hacker had no destructive nature. Their experiments with the digital space in combination with the emerging idea of selectivity and elitism resulted in diving into white and black or crackers. The latter are the major deviants in the digital environment and are engaged in obtaining unauthorized access to ITS and information. Hacktivists pursue political goals while hacking, stealing, disseminating confidential information and attacking critical infrastructure in cyberspace (Ovchinsky V. S., 2016: 193, 194). There are also so-called thrill-seekers who get satisfaction being a cyber threat actor and shows the lowest level of sophistication (Canadian Centre for Cyber Security).

So-called pirates either use programs developed by hackers or work on their own and can be classified depending on their functions: couriers and distributors. Taking the spam as an example, one may assume that database spammers create lists of user addresses and cracker spammers create programs that organize data, which describes couriers. In general, spammers generate and send unsolicited, intrusive advertising messages with hidden or false information to sell products, carry out phishing scams, distribute spy- and malware, or facilitate cyberattacks on organizations and, inter alia, mailing spammers or distributors are involved in sending spam.

Therefore, phishing is a popular cyberattack that uses e-mail or a malicious website to literally infect a computer with malware or collect sensitive information. E-mails often prompt users to open a link or attachment containing malicious code, after which the phisher gains access to the information contained in the device and takes control over the system. Malware includes viruses and ransomware, spyware and banking trojans (U.S. Small Business Administration).

Some attacks indicate that hacker organizations also pursue apolitical venal goals. For instance, the DarkSide group committed a cyberattack on the Colonial Pipeline on May 7, 2021. They encrypted 100 GB of data, having previously bought 740 GB of data from the French branch of Toshiba and gained access to administrative networks, subsequently blocking the toll collection system. 13 states had to declare state of emergency, which accounted for the transit of 45% of the consumption of the U.S. East Coast to 260 delivery points was suspended (about 3 million barrels per day). In 6 days, gas prices broke the record of the last 6 years (Bowcut S., 2021). The cyberattack affected

not only the filling stations, but also school classes, which had to be online. After the paying approximately 4.4 million US dollars in cryptocurrency (75 bitcoins), on May 13, 2021, operation was restored. The U.S. Department of Justice discloses that FBI succeeded in partial returning the ransom, but there is no data about accurate sum (63,5–66 bitcoins). In April 2021, in Pennsylvania, hackers almost dropped critical doses of cleaning chemicals into the water supply (in February a similar incident occurred in Florida) (Rspectr, 2021). In 2017, hackers broke into the computer networks of 10 U.S. power plants, including the Wolf Creek Generating Station in Kansas (Vadimova E., 2021). As a result, cybersecurity crimes have been seen as elements of terrorist activity (Lewis J. A., 2002).

Insiders are technical personnel who commit computer offenses, causing a failure in the ITS or stopping the production, or deforming the software. At the individual psychological level, the motives are venal intent (as to commercial spies) and sabotage and revenge (as to employees). The second phenomenon is more common (Dolgova A. I., 2020: 836). Their methods include the following groups. Firstly, legally reprogramming via a trojan horse, a computer virus and worm. Secondly, data illegal activity includes a salami slice which implies using a fake account to charge small sums and impersonation which involves unauthorized use of a user profile to get access. Thirdly, such programs as super-zapping and a logic bomb that either replaces anti-theft systems or adds additional app (Misbrener K., 2019).

In the considered sphere American criminologists classify the offenses into 3 categories. Firstly, cybercrimes as white-collar offense. Secondly, such Internet crimes distributing sexual material, DDoS, illegal copyright infringement, internet security fraud, theft, Ponzi or pyramid schemes, non-delivery of goods or services. Thirdly, computer crimes are theft of services and software, unauthorized use of computers, data usage for personal gain, virus or worm (Siegel L. J., 2006: 429–432). Classifying computer-related crimes, one should take into account what a computer constitutes: object (theft of hardware or software), subject (attempt to interfere with the services provided by computers.) and instrument (while committing traditional crimes) (Kim, C., Newberger, B., Shack, B., 2012: 443–488). British scholars also focus on the role of a computer: whether it is an instrument and an aim or complement to increase scale or area, but they used to other notions, inter alia, online harm, but it deals only with the harm suffered by individuals (Department for Digital, Culture, Media & Sport, 2020). Saudi Arabia stands for traditional division into crimes against people, property and government depending on object of a crime (Alabdulatif A., 2018). First violations include cyber harassment, stalking, distribution of children pornography, spoofing, fraud, human trafficking,

identity theft and libel or slander and attacks against ICS, SCADA, DCS. The second one involves DDoS, hacking, virus transmission, cyber and typo squatting, cyber-vandalism, copyright infringement and IPR violations. The third type covers nnauthorized access to essential information, hacking, hacktivism, cyberwar, cyberterrorism, pirated software.

It is also worth mentioning that the terminology is still developing. Although the notion of computer crime originally emerged in the early 60s (Volevodz A. G. 2002: 17). However, the foundations of the study were laid by Donn B. Parker in the early 80s (Shestak V. A., 2020: 3). He formulated such a specific term as computer abuse which implies computer use for improper or illegal activities. Subsequently Computer Fraud and Abuse Act of October 16, 1986 was adopted. Taking into account the U.S. current legal framework, the scholars distinguish five forms of computer misconduct: unauthorized access, unauthorized use, dishonest manipulation or alteration of data, sabotage, and theft of information. However, this classification is also not exhaustive and the terms cybercriminal and computer criminal may replace each other (Dzafarli V. F., 2021: 14).

Causes and Environmental Reasons for Emerging Cybersecurity Threats

A system of social factors and environmental reasons involves internal and environmental causes that may be defined as following: a cause is socio-psychological determinant that is developing in specific circumstances as accelerator, contributing to crime situation (Kuznetsova N. F., 2004).

Criminologists outline general and specific causes, objective and subjective approaches, social and economic factors, taking into account psychological phenomena that shape the modern model of human behavior. As for delinquency in general, reasons include the aspirations and skills of the individual withal a real opportunity to fulfil them through a device, the ease and availability of acquiring necessary knowledge and tools, community indifference or approval, antisocial behavior, as well as organizational, legal and technical defects of both particular companies and service providers. For instance, in 2019–2020 more than 33 thousand of users were hacked via Microsoft Exchange and Orion of SolarWinds. Half of the data was leaked. A similar incident occurred to Kaseya July 2, 2021, but it was immediately detected and prevented (Willett, M., 2021).

Scholars single out also economic reasons related to it: artificially inflating prices for software products, unfair trade and, as a result, obtruding malicious and anti-virus software. Such slow are the detection and adjustment that they constantly incur additional costs (Bailey T., Maruyama A., Wallance

D. T. 2020). Modernization and remote monitoring have always been and will be expensive. For instance, in order to keep updated, American local energy company has to spend more than 100 million of US dollars annually (Dwight L.J., Duke E., 2019).

Despite large offer of necessary programs to ensure the enterprise or company operation, the quantity is likely to fail to satisfy in terms of quality. Some vendors use unsecured computers or unproven technologies while developing applications and updates and neglect cybersecurity, believing that it is not their responsibility.

Some companies prefer to use specialized devices developed by startups due to limited funds. This issue has been deteriorating more and more during the pandemic. Often is a built-in security system in charge of proper operation, but they are not always capable to prevent large-scale incidents. Also, the using models of different generations and from different manufacturers reduces the data security and access to it, according to the Cybersecurity and Infrastructure Security Agency (U.S. Department of Homeland Security). The continuing decentralized nature of management exacerbates the deplorable state of the cybersecurity (Bailey T., Maruyama A., Wallance D. T. 2020).

Neglecting the physical security of critical infrastructure utilities, outdated or unreliable software, the lack of proper control over personnel and criteria for sensitive information or OPS and access to it, failure to provide mechanisms for non-disclosure of trade secrets are the specific circumstances. It is worth noting that green energy utilities are more vulnerable. Recent wind farm security studies show that physical vulnerabilities as an easy-to-pick padlock and lack of network security allow to take control over the entire wind farm network in minute. It results in damage 10–30 thousands of US dollars per hour (or 252–720 thousands of US dollars per day) or even complete destruction of the turbines (Staggs J. 2017).

Objective determinants are the disproportion between countermeasures and rapid development of crime, inadequate cost of maintenance and, as a result, the low security of the utilities, whereas the subjective ones include social and psychological deprivation, irresponsibility or permissiveness, global spread of radical ideologies such as violence, hatred, mass antisocial consciousness (Kleymenov M. P., 2018: 69).

Remote access and digital space limits feedback and makes it possible to take full advantage of anonymity. What gives rise high online criminal rate is such special conditions as greater accessibility of virtual objects, no need for active physical actions, a sense of permissiveness and impunity, remoteness from the victim. Thus, it causes aspirations of the individual and the possibility to introduce through an electronic device. On this ground cybercriminals less

fear of being detected and have confidence in being beyond the reach. The so-called crisis of conscience was noted as early as the 70s in the United States due to systematic everyday violence, rooted even during the campaigns to exterminate the American Indians (Schur, E.M., 1969).

Cyberspace is a perfect environment for hiding criminal activity and engaging a wider range of individuals who used to be less likely inclined to commit a crime. One may portrait cybercriminal personality by tracing the following stages:

(1) Deep dive in e-world in which anonymity reigns;
(2) Emerging phenomenon of virtual personality;
(3) Escapism and loss of identity;
(4) Internet addiction or behavioral addiction as a form of deviant behavior;
(5) Getting into a specific subculture of cybercrime.

As a result, cybercriminals quickly make a fortune, that is why such a way to earn is becoming enticing (Dzafarli V. F., 2021: 56–60, 65, 85, 96–99).

Cybersecurity crime is often characterized by high latency or even ultra-high latency. Some researchers treat it as a means of achieving such inimical consequences as damage to national interests, crashes, environmental disasters, deaths or injuries and economic loss, thus encroaching on various objects of crime. They can be either organized or transnational, or local (Dolgova A. I., 2020: 831–833).

CONCLUSIONS

In conclusion, a cybersecurity threat is a complex phenomenon that includes any circumstance, condition and event that jeopardizes the object of the attack via the ITS, computer system or network through unauthorized access, destruction, disclosure, data modification and/or denial of equipment and results from (in)actions. Actions is responsibility of an offender, whereas apathy untimely response accounts for a victim. Unfortunately, it is impossible to consider in detail all the classifications of cybersecurity threats, however, authors have given a general description of particular types of the cyber threats and summarized it in Appendix B. Not only do incipient technologies change the social co-existence and complicate human interaction but are involved in evolving innovative crime and brand-new threats. Exacerbation of the criminogenic situation roots from a range of elements of an individual's social structure in interaction with the environment that have been examined by the authors.

At first, there was a lack of proper control, low security of the object of criminal encroachment, lagging counteraction. The intensive improvement of the various methods to commit a crime led to the failure to take sufficient measures in time. In order to ensure the security of operated computers, their systems and networks it would have taken too high costs. The lack of special units in law enforcement bodies also boosted crime situation in digital space. The more advanced technologies appear, the more sophisticated crimes become and more skilled personnel is on demand. Despite the efforts, a gap between the prevention measures and cyber criminality remains. On these grounds cybersecurity threats are one of the most acute problems throughout the world and should be studied more thoroughly.

REFERENCES

Alabdulatif, A. (2018). *Cybercrime and analysis of laws in Kingdome of Saudi Arabia*. [Master of Science in Information System Security, Technology of University of Houston]. Available at: https://uh-ir.tdl.org/bitstream/handle/10657/3107/ALABDULATIF-THESIS-2018.pdf?sequence=1.

Bailey, T., Maruyama, A. & Wallance, D. (2020). *The energy-sector threat: How to address cybersecurity vulnerabilities.* McKinsey & Company, 2020. Available at: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities.

Desarnaud, G. (2017). *Cybersecurity attacks and energy infractutures. Anticipating Risks.* Études de l'Ifri. Available at: https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf.

Belous, A.I. (2020). *Cybersecurity of fuel and energy complex facilities.* Concepts, methods and tools for ensuring. Moscow, Vologda: Infra-Inzheneriya.

Black Kite (2021). *The 2021 ransomware risk pulse:* energy sector. Ransomware on the Rise Across Critical Infrastructure. Available at: https://blackkite.com/wp-content/uploads/2021/09/The-2021-Ransomware-Risk-Pulse-_-Energy-Sector.pdf.

Bowcut, S. (2021). C*ybersecurity in the energy industry.* Cybersecurityguide. Available at: https://cybersecurityguide.org/industries/energy/.

Canadian Centre for Cyber Security. N*ational Cyber Threat Assessment.* An Introduction to the Cyber Threat Environment. Available at: https://cyber.gc.ca/sites/default/files/cyber/publications/Intro-ncta-2020_e.pdf.

CISA. *Bad Practices.* Available at: https://www.cisa.gov/BadPractices.

Department for Digital, Culture, Media & Sport (2020). *Online Harms White Paper 2020*. Available at: https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

Duke Energy. (2019). *Accounting request related to cybersecurity informational technology–operational technology program*: letter to Kimberly D. Bose, US Federal Energy Regulatory Commission No. AC19-75-000. Available at: https://www.federalregister.gov/documents/2019/03/22/2019-05482/duke-energy-corporation-notice-of-filing.

Dolgova, A.I. (2020). *Criminology*. Moscow: Norma.

Dzafarli, V. F. (2021). *Criminology of cybersecurity: Criminological means of crime prevention in the field of information and communication technologies*. (S. Ya. Lebedeva, Ed.). Moscow: Prospekt.

IT Governance. *What is Cyber Security?* Definition and Best Practices. Available at: https://www.itgovernance.co.uk/what-is-cybersecurity.

Kaspersky, E. (2017). S*toneDrill:* We've Found New Powerful 'Shamoon-ish' Wiper Malware – and It's Serious. Official Blog of Eugene Kaspersky. Available at: https://eugene.kaspersky.com/2017/03/06/stonedrill-weve-found-new-powerful-shamoon-ish-wiper-malware-and-its-serious/.

Kaspersky Laboratory (2020). *Kaspersky Security Bulletin.* Statistics 2020. Available at: http://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_ru.pdf.

Kim, C., Newberger, B. & Shack, B. (2012). Computer Crimes. *American Criminal Law Review.* 49(2), 443-488.

Kleymenov, M. P. (2018). *Criminology*. Moscow: NORMA.

Kovacs, E. (2018). *Shamoon 3 Attacks Targeted Several Sectors.* Security Week. Available at: https://www.securityweek.com/shamoon-3-attacks-targeted-several-sectors.

Kuznetsova, N. F. (2004). *Criminology*. (N. F. Kuznetsova, V. V. Luneev, Ed.). Moscow: Wolters Kluwer.

Livingston, S., Sanborn, S., Slaughter, A., Zonneveld, P. (2019). *Managing cyber risk in the electric power sector.* Emerging threats to supply chain and industrial control. Deloitte. Available at: https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf.

Lewis, J. A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats Center for Strategic and International Studies.* Washington, D. C.

Misbrener, K. (2019). *Cyberattacks threaten smart inverters, but scientists have solutions.* Solar Power World. Available at: https://www.solarpowerworldonline.com/2019/04/cyberattacks-threaten-smart-inverters-but-scientists-have-solutions/.

Nescout. (2021). *Threat Intelligence Report 2021*. Available at: https://www.netscout.com/threatreport.

National Institute of Standards and Technology (NIST). *Cyber Attack*. Available at: https://csrc.nist.gov/glossary/term/cyber_attack.

National Institute of Standards and Technology (NIST). *Cyber incident.* Available at: https://csrc.nist.gov/glossary/term/cyber_incident.

National Institute of Standards and Technology (NIST). *Cyber Security.* Available at: https://csrc.nist.gov/glossary/term/cyber_security.

National Institute of Standards and Technology (NIST). *Cyber Threat.* Available at: https://csrc.nist.gov/glossary/term/cyber_threat.

National Institute of Standards and Technology (NIST). *Cybersecurity.* Available at: https://csrc.nist.gov/glossary/term/cybersecurity.

National Institute of Standards and Technology (NIST). *Cybersecurity event.* Available at: https://csrc.nist.gov/glossary/term/cybersecurity_event.

National Institute of Standards and Technology (NIST). *Cybersecurity Incident.* Available at: https://csrc.nist.gov/glossary/term/cybersecurity_incident.

National Institute of Standards and Technology (NIST). *Cyberspace*. Available at: https://csrc.nist.gov/glossary/term/cyberspace.

National Institute of Standards and Technology (NIST). *Cyberspace attack.* Available at: https://csrc.nist.gov/glossary/term/cyberspace_attack.

Ovchinsky, V. S. (2016). *Criminology of the Digital World*. Moscow: Norma. INFRA-M.

Petcu, A. G. (2022). *Emotet Malware Over the Years: The History of an Infamous Cyber-Threat.* Heimdal security. Available at: https://heimdalsecurity.com/blog/emotet-malware-history/.

Rspectr. (2021) *Bulk encryption weapons.* Available at: https://www.rspectr.com/articles/828/oruzhie-massovogo-shifrovaniya.

Schur, E. M. (1969). *Our criminal society:* the social and legal sources of crime in America. New Jersey: Prentice-Hall.

Shestak, V. A. (2020). Foreign experience in the legal regulation to counter cybercrime. SSRN, 2020 *Criminal Law:* development strategy in the XXI century. Materials of the XVII International Scientific-Practical

Conference, 23.01-24.01.2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524513.

Siegel, L. J. (2006). *Criminology*. Thomson Wadsworth.

Staggs, J. (2017). *Adventures in attacking windfarm control networks*. Black Hat USA. Available at: https://www.blackhat.com/us-17/briefings/schedule/#adventures-in-attacking-wind-farm-control-networks-6394.

U.S. Small Business Administration. *Stay safe from cybersecurity threats.* Available at: https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats.

Vadimova, E. (2021). Digital against Fuel and energy complex. *Oil and Capital*. Available at: https://oilcapital.ru/article/general/29-06-2021/tsifra-protiv-tek.

Volevodz, A. G. (2001). *Combating computer-related crime:* the legal framework for international cooperation. Moscow: Yurlitinform.

Willett, M. (2021) Lessons of the SolarWinds Hack. *Survival*. 63(2): 7-26.

World Economic Forum. (2021). *The Global Risks Report 2021*. Available at: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET