Avramov S. Arseniy Master of law

Synergy University

arseniyavramov@gmail.com

Volkova A. Maria Ph.D. associate professor

Synergy University

mvolkova2013@bk.ru

CYBER ATTACKS ACROSS THE WORLD, INVESTIGATING AND DEALING VS, LEGAL AND TECHNOLOGICAL CHALLENGES

Abstract

The twenty first century is often called the century or even the era of technology, where people meet all kinds of technology in every minute on a daily basis. It starts from a usual worker's smartphone and ends up in larger scale, where some massive companies' software is simply doing its job and yet can meet a not very simple issue – called cyber attack. Cyber attacks have been existing for some years now, but just like technology, they grow and evolve into something bigger, as nowadays they are usually not just a "little hack", as they became big on a national and international levels and they are exactly like that this article will investigate.

Keywords: cyber attack, security, internet, modern situation, cyber crime

1. Introduction

Cyber attacks can affect the information space in which the resources of a physical device are concentrated, it usually requires verification of data carriers, specifically designed for their storage, processing and transmission of the user's personal information (Z Zhesterov, P.V. 'From visible past to an invisible presence: new criminological reality after planetary cyber attack 12/05/17 WannaCry', East European Review, 2018, volume 9, issue 2, pp. 57). The most common kinds of cyber attacks include: DDoS attacks, which are distributed denial of service attacks that are implemented by using several compromised computer systems as sources of attack traffic, they flood systems with a large number of requests, resulting in reduced throughput and systems becoming overloaded and unavailable, bots, that are software robots who mimic or replace human behaviour and perform simple tasks at a speed that exceeds user

activity, as well as fishing and brute force, where attackers use apps and scripts as “brute-force tools” that try multiple password combinations to bypass authentication processes. The main targets of cyber attacks are credit and financial sector, public authorities, defence industry and space, science and education and others, where the obvious goals are to either steal information and money or to make the processes work much worse than at the base level. It is very tough to fight against cyber attacks, and it is indeed extremely hard to actually find those “attackers” in real life, since they do everything in their power to secure their “irl” (*in real life*) location (Kobets, P.N. – Krasnova, K.A. Criminal-legal measures to ensure cyber security in the conditions of exponent growth of cyber-crime. In the collection: Ensuring public safety and combating crime: tasks, problems and prospects. Materials of the All-Russian Scientific and Practical Conference in 2 volumes. Krasnodar, 2017, p.207). By knowing all of those information some questions appear: How do governments fight against it? How do countries classify cyber attacks from the perspective of legislation?

2. Methods around the world and the legislations of fighting against cyber crimes

Let us try to figure out the answers to those questions in various countries.

In the U.S.A. for instance, on 14th February 2003 there was a publication of the "National Cyber Security Strategy, which became part of the "National Strategy for the Physical Protection of Critical Infrastructure and Key Assets" (Kovaleva T.K.Critical Infrastructure in the US // National Security innovation and investment. 2019. P.81). The American authorities recognized that the country's infrastructure completely depended on information systems and networks that were vulnerable to external cyber attacks. The main goal of the strategy was the creation of a unified national system for responding to such attacks.

In May 2011, the "International Strategy for Action in Cyberspace" (https://medialaw.asia/node/9003) was published in which it announced its readiness to use military means to neutralize threats in the information space. In July, the Pentagon's own cyberspace strategy became known (The Computer Fraud and Abuse Act (USA-CFAA), 18 U.S.C. 1030.). By using legal steps, the US has put up sanctions for cybercrime that include monetary fines and imprisonment. The punishment depends on many factors: the severity of the crime committed, the amount of economic damage caused by the act, the defendant's criminal past, and many others. Currently, the US Congress is considering a new law on cybersecurity, which provides tougher penalties for cybercrimes and the actual equalization of the definition of their public danger with real crimes.

In February 2011, the *German* government adopted the "Cyberspace Security Strategy", which sets goals for increasing the cybersecurity of government structures, the economy and private users (https://digital.report/kibergotovnost-germanii-2-0-natsionalnaya-strategiya/). In the German strategy, just like in the American one, the secret part remains unknown, apparently concerning the system of countermeasures against information attacks. Considering the legal part, the German Penal Code uses a special term – "Daten", which is defined in article 202 of the German Criminal Code – data that is stored or transmitted electronically, magnetically or in another way that is not directly visually perceptible, i.e. computer data. Illegal receipt by a person of computer data that was not intended for him, which is under special protection against unauthorized access, in order to gain benefits for himself or for a third party shall entail imprisonment for up to three years. Erasing, destroying, rendering unusable, altering data or attempting to do so is punishable by a fine or imprisonment for up to two years. Paragraph "B" of article 303 of the Criminal Code covers such crimes as DNS attacks (computer sabotage) and the creation of malware (Federal Ministry of Justice (Ger), Prof. Dr. Michael Bohlander). The article contains a provision that computer sabotage - interference with the processing of data that is essential to a business, government agencies, or someone else's way of doing business, is a crime. Interference can be carried out by destroying, damaging, rendering unusable, altering a computer system, or interfering with data transmission. These acts are punishable by imprisonment for up to five years.

In the *Netherlands*, "*the intentional use of technical devices for intercepting or recording data flowing through telecommunication systems or connected equipment, for the purpose of deriving benefit for himself or for a third party, if the data is not intended only for him, provides for a fine or imprisonment for up to 1 year*" states Article 139c of the Criminal Code. While *"a person who provides the means to unlawfully intercept and record data flowing through telecommunications or automated systems may be subject to a fine or imprisonment for up to 6 months"* (Article 139d) (Die Verfassung des Königreichs der Niederlande, 2018). In 1993, the Netherlands adopted the Law on Computer Crimes, supplementing the Dutch Criminal Code with new compositions: unauthorized access to computer networks; unauthorized copying of data; computer sabotage; the spread of viruses; computer espionage. Additions and clarifications were made to a number of articles of the Dutch Criminal Code that provide for liability for committing traditional crimes (extortion, fraud, forgery, etc.), which allows using these elements of crime, in appropriate cases, to combat computer crimes.

Similar documents have been adopted in Great Britain and India.

In the Russian Federation, the situation with qualified personnel in the field of cybersecurity in Russia is rather the same as in the United States, but has more acute character. Therefore, it is proposed to introduce and develop special courses on the investigation of such crimes at law faculties in the field of telecommunication technologies, cybersecurity and information security. Russian professors think that it is necessary that every graduate of the Faculty of Law possess not only legal knowledge, but also proper digital literacy (Zhurmukhambetova 2021). It is necessary to improve the digital literacy of the population in order to avoid the emergence of new cybercrime, to develop this literacy among law enforcement officers in order to prevent cybercrime. Without a proper regulatory framework, there can be no effective fight against cybercrime by law enforcement agencies. The fact that the state is pursuing an active policy is not denied to solve the above problems. However, at the moment the intensity of the development of this issue is still insufficient. According to the Ministry of Internal Affairs, over the period of 2020, the number of crimes committed using information and communication technologies has increased by 94.6%, grave and especially grave – by 129.7%. It should be noted that payment cards for criminal purposes were actually used 6 times more often than in 2019, when there was no danger of a pandemic, and mobile communications were used for the same purposes 2 times more often and more. According to statistics on cybercrime, for example, the Bryansk prosecutor's office for 2019 indicated that 1372 crimes were committed using information and telecommunication technologies, which is almost 2 times more than in the same period in the past (Ministry of Internal Affairs of the Russian Federation^ Brief description of the state of crime in Russia, 2020).

3. The COVID-19 and 2022 situations' impact on cybercrimes

The COVID-19 pandemic has made significant changes in the life of all (Reshnyak, M.G. – Botasheva, Z.H. Addressing some of the legal challenges posed by the coronavirus infection control system (COVID-19), Gaps in Russian legislation, 2021, volume 14, number 4, p269; Krasnova, K.A. – Topilskaya, E.V. Pandemic is not a barrier for student science. In the collection: Cybercrime: risks and threats, materials of the all-Russian student round scientific and practical table with international participation. St. Petersburg, 2021. p. 9). First of all, those changes are associated with various kinds of restrictions, like the cancelling of mass events, compliance with masks and gloves regime and social distancing. Talking about the situation in Russia, due to the fact that a huge number of citizens were ordered to stay at home, the load force on the internet has been very significant. As a result, there have been multiple interruptions in the internet connection for a long time. At the moment on one hand, scammers

have become more active and have begun to act even more sophisticated than before the pandemic. Both the internet service providers and the ordinary users were not ready for such global changes in their lives and activities, so the attackers took advantage of this.

Government forces have tried to fight against it, but who was ready for such a powerful shot? It is unacceptable to assume that law enforcement agencies and representatives of state structures did not take any action. On the contrary, they did in fact respond very quickly to any offenses in the area related to information and communication services. Moreover, long before that, in order to implement preventive measures, Russia during the 74th session of the United Nations proposed, under the auspices of the UN, agreed on and approved a convention on combating crimes in the field of the use of information and communication technologies, which would allow for effective international cooperation in the field of combating cybercrime. Analysing this situation, we can conclude that in addition to strengthening legal regulation, the main method of combating cybercrime is to increase the legal culture of the population, including educating citizens in the field of computer literacy. The fact is that one of the most frequently committed crimes on the Internet is extortion, including personal data. And if citizens are warned about the danger of providing their data and other actions by which fraudsters can deceive them, then the number of crimes in the corresponding category will significantly decrease. Unfortunately, with all the varieties of legal instruments, available to public authorities, at the moment there are still some difficulties in their application to combat the activities of criminal elements in the internet websites. At the same time, the leadership of the authorized bodies of state power is taking a lot of efforts to optimize the organizational structure and increase the efficiency of their work, which is a prerequisite for systematic and efficient activities to prevent and combat cybercrime. In the light of these arguments, it is impossible not to mention Mikhail Mishustin reforms of the state apparatus. As part of its implementation, the staff of civil servants in central and territorial government bodies will be optimized, which, as the Head of the Government Staff Dmitry Grigorenko notes, will allow the public administration system to become “more clear, logical, up-to-date” (Countering the use of information and communication technologies for criminal purposes // United Nations Office on Drugs and Crime, 2019).

Russian newspaper “Izvestie” tells its readers about many cyber crimes happening on a daily basis, starting from February of 2022. Apart from the propaganda from both sides, it is very clear that “special military operation” happens not only at the battlefield of both ground and skies, but on cyber level as well. It is almost impossible to find the truth, therefore it is understandable that several acts are happening big and small providing its impact. According

to “Izvestie” Ukrainian hackers have launched a large-scale attack on the “Mir” payment system and its operator, the National Payment Card System (NSPK). This was reported on September 23 by the Kommersant newspaper, citing its source in the field of information security. “The goal of the attack is to overload the system and cause a failure in card servicing. Since the beginning of the military operation in Ukraine, the entire Russian IT infrastructure has been subjected to massive hacker attacks. Until now, there has been no information about vulnerabilities in the Mir system”, the newspaper says. Cyber activists generate traffic to systems using browsers or primitive DDoS tools to disrupt payments and terminals. The source of the newspaper has also noted that in the current situation, the attackers may be able to succeed in the attacks. In this case, it is possible to disable cashless payments for several hours. The Ministry of Digital Development reported that this issue is within the competence of the National Coordination Centre for Computer Incidents, as well as within the competence of the Central Bank. However, at the moment, representatives of the Central Bank did not answer the newspaper, and the NSPK declined to comment. Earlier that day, Sergei Solovykh, head of the department for working with wealthy clients at Fontvielle Investment Company, told Izvestia that the topic of using “Mir” payment cards had become speculative abroad, since it had more political overtones than economic ones. On the same day, the United States was threatening to impose sanctions on those Turkish credit organizations that would continue to work with the Mir payment system. According to the Turkish media, the banks most often used by “Mir” card holders in Turkey continue to work with them. Earlier in September, some hotels in Turkey stopped accepting payments through Mir due to the threat of sanctions. One of the major chains confirmed that since September 15, it was recommended in the country not to accept cards, but each hotel can decide for itself whether to follow these recommendations or not. This is just a fresh example of many cyber crimes happening right now. From the scientific point of view, it is hard to find the right thing to do, especially from the legal perspective.

Conclusion

In such circumstances and conditions, it is rather necessary that the legal regulation of cybersecurity is carried out not only at the regional level. Safety efficiency can only be achieved through the unification of international and foreign norms, which will grant a better result. At the same time, it would be right to carry out more detailed regulations of all areas of public relations, such as: property, advertising, information, financial and other areas.

References

Dolgopolov, A. 'Impact of the COVID-19 pandemic on cybercrime'. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp.13-16.

Kobets, P.N. – Krasnova, K.A. 'Criminal-legal measures to ensure cyber security in the conditions of exponent growth of cyber-crime'. In Ensuring public safety and combating crime: tasks, problems and prospects. Materials of the All-Russian scientific and practical conference in 2 volumes. Krasnodar, 2017, pp. 205-208.

Kovaleva, T.K. 'Critical Infrastructure in the US'. National Security innovation and investment, 2019, pp. 78-85.

Krasnova, K.A. – Topilskaya, E.V. 'Pandemic is not a barrier for student science'. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. St. Petersburg, 2021, pp. 8-10.

Reshnyak, M.G. – Botasheva, Z.H. 'Addressing some of the legal challenges posed by the coronavirus infection control system (COVID-19)', Gaps in Russian legislation, 2021, volume 14, number 4, pp. 266-270.

Prashant, M. Classification of Cyber Crimes, LCI, 2020.

Synkov, V.V. 'Cybercrime is the challenge of the 21st century'. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp.208-212**.**

Tamrazov, G.O. 'Fraud in the field of computer information: qualification problems'. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp. 63-68.

Voinov, N.E. 'Cybercrime in the Russian Federation: current state and current problems'. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp.142-147.

Zhesterov, P.V. 'From visible pasts to an invisible presence: new criminological reality after planetary cyber attack 12/05/17 WannaCry', East European Review, 2018, volume 9, issue 2, pp. 55-67.

Zhurmukhambetova, S. 'Cybersecurity Trends in the fight against cybercrime'. In Cybercrime: risks and outliers. Materials of the All-Russian student round scientific and practical table. Edited by E.N. Rakhmanova. St. Petersburg, 2021, pp.167-172.