Published by the decision of the Scientific Council of
The Institute of Philosophy, Sociology and Law of NAS RA

The POLITNOMOS
Journal of Political and Legal Studies

1(1), 2023

YEREVAN - 2023

POLITICAL STUDIES, POLITICAL PHILOSOPHY

CYBER-SECURITY AS THE MOST IMPORTANT COMPONENT OF NATIONAL SECURITY

Narine Aghayan, Junior Researcher
Institute of Philosophy,
Sociology and Law of NAS RA
(Email: nana.aghayan@gmail.com)

Abstract

Information and communication technologies (ICT) are developing rapidly in the world. Not yet adapted to the first wave, there is a need to follow and master the next ones in order to keep up with the demands of the time. Their influence in our time is very significant in all major spheres of activity of citizens, organizations, and the state. The opportunities offered by the Internet and cyberspace create broad prospects for the development of the political, economic, defense, and other spheres of the state. However, at the same time, the dangers and threats in the above-mentioned and all other areas are increasing dramatically.

Keywords: cybercrime, information technologies, information security, cyberterrorism, cyber threats, cyberspace, cyber-security strategy.

The cross-border nature of cyberspace, its dependence on complex information technologies, active use of virtual space platforms and services by various groups of citizens cause new risks in terms of violating the interests of the individual, organization, and state (Danenyan, 2020, 261-269).

In the 21st century, for the first time, humanity faced a new, previously unknown type of crime: cybercrime. "Cybercrime is based on the hacking of web pages, malicious software, and the distribution of illegal information by people or groups who carry out criminal activities in the virtual space using information technologies" (Timofeev, Komolov, 2021).

The growth of cybercrime in the world proves that cyber threats on the Internet are growing more and more and pose serious threats to the national security of states (Atoyan, 2014, 154). The development of cyber-attacks follows the rapid pace of information technology development, resulting in the refinement of similar attacks and changes in methods and means of execution. That the mentioned threats are not at all exaggerated, the clearest evidence of this is the increasing number and quality of hacking attacks on various Internet resources, local networks, data warehouses, and government organizations. According to UN experts, the economic damage from cybercrime has reached 3 trillion dollars by the beginning of 2021 (UN, 2021).

There are hacker groups operating in about 130 countries that develop millions of new malicious programs every month and carry out several hundred million cyberattacks every year (Allianz Global Corporate & Specialty). Their purpose is to cause financial and economic damage to "conditional opponents", competing business organizations, or to get personal profit. The Council of Europe Convention on Cybercrime (this convention entered into force in the Republic of Armenia in 2007) divides it into five groups.

The first group includes "computer crimes" directed against the confidentiality, integrity, and availability of computer data and systems. Among them are illegal access, illegal acquisition of information, data tampering, system tampering, etc.

The second group includes illegal acts using computer means, among which are frauds using computer technologies, frauds for economic gain, etc.

The third group consists of crimes related to content orientation, primarily the promotion of child pornography.

The fourth is copyright and other rights violations.

The fifth group includes the following crimes: dissemination of racist and similar information that incites violent actions, incites hatred, and discrimination against any person or group of persons based on their national, racial, or religious affiliation (The Council of Europe Convention on Cybercrime, 2001).

Cybercriminals take advantage of countries' legislative loopholes and inadequate security measures. The poor state of computer literacy and so-called "computer hygiene" also creates fertile ground. Lack of cooperation between developed and developing countries is also a favorable condition for cybercriminals (UN, 2021).

Given that most of the daily activities of citizens, countries, and states in the modern world are managed through networks and programs, this significantly increases their vulnerability to cyber-attacks.

For example, currently, electronic document circulation, state population register, social security sector, real estate registration, tax reporting, and a number of other systems are widely implemented in RA, the failure of which may lead to a temporary blocking of the implementation of the most important functions of the state, which in turn will lead to other related areas of paralysis. All this is also fraught with threats to the national security of countries, among which cybercrime is the largest in volume. It is one of the fastest-growing types of transnational crime.

From what has been said, it follows that the fight against various manifestations of virtual crimes is imperative at the national level, so it is necessary to have an educated, literate, and knowledgeable society in this regard. Developing and implementing appropriate educational programs to develop media literacy in the field, teaching them from junior school age, as well as conducting public awareness events can contribute to solving this problem. Media literacy is, first of all, the ability to distinguish information sources, to perceive the large amount of information that is exported to the virtual space, and to distinguish the true from the false. Proponents of media literacy education are convinced that including media literacy in school programs promotes children's civic engagement and helps them acquire critical and investigative skills.

Currently, there is a huge amount of information on the Internet, so it is very easy to be deceived and confuse fake with reliable information. Computer fraudsters and fraudsters take advantage of the fact that in this variety and abundance of information, as well as due to lack of time, users are often misguided and take actions without checking the information, which leads to negative results or irreparable consequences for them.

Media literacy training aims to raise awareness of the impact of mass media, social networks, and various sources and to form an active stance toward both the use of information sources and their creation.

Media literacy is one of the important components of the content of education today. Taking into account the importance of the issue, under the leadership of UNESCO, Media Literacy Week has been held in different countries of the world in recent years, with various educational programs and events. Fortunately, steps have been taken in this direction in the field of education of the Republic of Armenia.

In 2013, the "Media Literacy" manual for teachers, guaranteed by the Ministry of Education and Culture, was published. It is the first Armenian-language guide for teachers, which also contains digital games and audio-visual materials. It helps to understand and communicate to young people how the media sphere works, how to navigate modern information flows, and critically consume any Internet product. Starting in 2017, the Ministry of Education, Science, Culture and Sports of the Republic of Armenia, together with various organizations and supporters, organizes an educational week in the schools of Armenia every. In addition, various events and open classes, video and film viewings, and discussions are organized. Perhaps, over time, teaching media literacy as a separate subject in school curricula will become necessary. With these steps, children will be better prepared to avoid various virtual traps and pitfalls as they enter adulthood.

With the growing trends of cybercrime in front of our eyes, there is no doubt that cybersecurity is becoming an important component of not only personal but also national security. In the case of Armenia, the special services of a number of unfriendly countries, especially Azerbaijan and Turkey, pose a serious threat. As a result, thousands of Armenians and Diaspora Armenians are continuously suffering from the actions of Azerbaijani-Turkish hackers. The history of cyber wars between Armenia and Azerbaijan begins in 2000 when the Internet was not practically developed in both countries, there were several dozens of websites, and the number of Internet users was not particularly large. At that time, a number of websites were hacked on both sides. 2006-2007 Azerbaijani hackers started to become active again, forming groups attacking Armenian websites, which were engaged in spreading insults to Armenians and propaganda materials of anti-Armenian nature. During that period, the attacks were mostly one-sided. The point is that the field of information security in Armenia was so neglected that state websites were also often hacked. Cases of leakage of information from state institutions were also recorded. The situation started to change in 2009 from the second half, when the control of the state sector of the Armenian network was placed on the National Security Service of Armenia. It is true that parallel to this, the number of attacks against the private sector of the Armenian network has increased. After that, until 2016 no attacks with serious consequences were reported. On January 19-20 of this year, the websites of RA embassies were subjected to a massive hacking attack, in response to which Armenian hackers hacked the blogs of 16,000 users of Azerbaijan (PanArmenian, 2016).

During the April four-day period of 2016 and the days close to it, Azerbaijani cyber-attacks intensified sharply, and in solidarity with them, Turkish hackers also became active. In response, Armenian hacking groups were active, in particular hacking the website of the government of Azerbaijan and publishing the personal data of 25,000 soldiers of the armed forces of that country. Since the April war, Azerbaijani hackers have increasingly targeted Armenian Facebook users, hacking profiles, emails, and Facebook account logins, among others.

Azerbaijan's hacker teams have been dramatically active since the summer of 2020, even before the military clashes on the border of Tavush (July 12-16). During June and July, tens of thousands of people's personal data were leaked as a result of targeted attacks by Azerbaijani hacking teams.

On July 14 of the same year, Azerbaijani hackers launched a cyberattack on the official websites gov.am, e-gov.am and primeminister.am. In response, one of the Armenian hacking teams launched an attack and hacked WiFi devices of nearly two thousand households and offices in Azerbaijan, changing their DNS settings.

Already during the 44-day Artsakh war, Azerbaijani hackers managed to hack a number of state websites, as well as infiltrate the system of circulation of state documents, take over the e-mails of a number of high-ranking officials, etc. In addition, a number of media outlets were hacked, and almost the entire media and government sector was under continuous and powerful DDoS attacks (Sputnik Armenia, 2020).

Considering the importance of the problem, certain steps have been taken in the last decade and a half in RA.

The National Assembly of the Republic of Armenia in 2007 ratified the Council of Europe Convention "On Cybercrimes" and the additional protocol of the same convention "On the criminalization of acts of a racist and xenophobic nature committed through computer systems" (Arlis, 2001).

In 2009 the concept of information security of the Republic of Armenia was adopted (MFA of RA, 2009), in which the types of threats to the information security of the Republic of Armenia were formulated, among which cyber terrorism is also included, and the priority measures to counter them and the priorities of their implementation were noted.

The national program for increasing the effectiveness of the fight against organized crime in the Republic of Armenia (2011) also aims to ensure cyber security (Arlis, 2011). Taking into account the growing trends of cybercrime, in 2012 the national strategy for combating terrorism in the Republic of Armenia was adopted (Arlis, 2012). Here, cyberterrorism is clearly defined as a "variety of terrorism".

In the following years, further steps were taken to bring the RA legislation related to this field into line with the requirements of international law and existing conventions, realizing that the emergence and use of the newest means of information intervention in the world continuously create new threats and will continue to create them in the future, therefore, there is a need to quickly respond to them theoretically, legal, constantly improve the legal bases.

The project of information security assurance and information policy concept was developed. It was approved by the National Security Council on 27.09.2017 in the session. 2017 At the end of the year (20.12.2017), the Government of the Republic of Armenia developed a draft Cyber Security Strategy and the schedule of measures arising from it (E-Draft, 2017). Many countries have such strategies, as their need arises from the need for safe and reliable operation of infrastructure in physical and virtual spaces. Taking into account the speed and unpredictability of current geopolitical developments, it is necessary to amend and adopt the above-mentioned bill, defining the priorities, principles, and measures to be implemented in the field of internal and external policy of the Republic of Armenia. The strategy should consider cyberspace as a clearly defined part of the information space. This approach is consistent with international standards, which define "cyber security" as a narrower concept than "information security".

Thus, these two concepts, despite many similarities, should not be equated, but should be considered separately, so cyberspace in the cyber security strategy should be defined as a specific field of activity in the information space.

Currently, the issue of creating a strategic research center for cyber security under the auspices of the state is also relevant, where mechanisms and models for combating cybercrime will be developed at the level of scientific and theoretical research, which will be used by both state departments and private companies. By the way, there is a relevant chapter (Chapter V) on this in the above draft Cyber Security Strategy.

The fight against cybercrime is a challenge both worldwide and in Armenia. This struggle cannot be effectively organized without the presence of a qualified and knowledgeable society. The best way to solve this problem is to develop and implement appropriate educational programs for the development of the sector, as well as to hold public awareness events.

Conclusion

In the 21st century – humanity first encountered a new type of crime – cybercrime. Cross – border nature of cyberspace, its dependence on complex information technologies, the active use of virtual platform and services by various groups of citizens creates new risks in terms of violating the interests of individuals, organizations and states. The growth of cybercrime in the world indicates that cyber threats on the Internet will increase and create even greater threats to the national security of states. Given the speed and unpredictability of current geopolitical even, it is necessary to have a cybersecurity strategy in the Republic of Armenia, which will define priorities, principles and measures implemented in the field of domestic and foreign policy. At present, the issue of creating a center for strategic research on cybersecurity under the auspices of the state is also relevant, where mechanisms and models for combating cybercrime will by developed at the level of scientific and theoretical research, which will used by both government departments and private companies.

References

Adrbejani haqernery kotrel en HH despanatneri kayqery (Azeri hackers hacked the websites of RA embassies, in Armenian). Retrieved May 2, 2023 from: http://www.panarmenian.net/arm/news/204165/

Allianz Global Corporate & Specialty. Retrieved March 15, 2023 from: http://www.agcs.allianz.com/

Atoyan, V. K. (2014). *Azgayin anvtangutyan himnakhndirner* (Issues of National Security, in Armenian). Yerevan.

Danenyan, A. (2020). *Mezhdunarodnoe pravovoe regulirovanie kiberprostranstva* (International Legal Regulation of Cyberspace, In Russian), Education and Law, 1, 261–269.

Hayastani Hanrapetutyan azgayin anvtangutyan razmavarutyun (National Security Strategy of the Republic of Armenia, in Armenian). Retrieved February 25, 2023 from: http://www.mfa.am/u_files/file/doctrine/Doctrinearm.pdf

Hayastani Hanrapetutyunum kazmakerpvac hantsavorutyan dem payqari ardynavetuyan bardzracman azgayin cragir (National program for increasing the effectiveness of the fight against organized crime in the Republic of Armenia, in Armenian). Retrieved April 8, 2023 from: http:/www.arlis.am /documentview.aspx?docid=73264

Hayastani Hanrapetutyunum ahabekchutyan dem payqari azgayin razmavarutyun (National Strategy against Terrorism in the Republic of Armenia, in Armenian). Retrieved January 18, 2023 from: http://www.arlis.am/DocumentView.aspx?DocID=75353

HH karavarutyan "Kiberanvtangutyan razmavarutuny hastatelu masin" ardzanagrayin voroshman nakhagits (Draft protocol decision of the RA government "On approving the cyber security strategy", in Armenian). Retrieved May 6, 2023 from: https://www.e-draft.am/projects/581/about

Kiberhantsavorutyun (hamakargchayin texekutyunneri anvtangutyan dem uxxvac hantsavorutyun) (Cybercrime, crime against the security of computer information, in Armenian). Redrieved April 21, 2023 from: http://www.un.am/up/file/Crime%20Congress_Cybercrime_Arm_Final.pdf

Konventsiya kiberhantsagortsutyan masin (Convention on Cybercrime, in Armenian). Retrieved February 12, 2023 from: http://www.arlis.am/DocumentView.aspx? docid=48028

The Council of Europe Convention on Cybercrime. Retrieved May 1, 2023 from: www.coe.int/t/DC/Files/Source/FS_cybercrime_ru.doc

Timofeev, A. V. & Kimolov, A. A. (2021). *Kiberprestupnost kak sotsialnaya ugroza i obyekt pravovovo regulirovaniya* (Cybercrime as a social threat and object of legal regulation, in Russian). Bulletin of Moscow State Regional University. Philosophical Sciences, 1, 95-101.

Voch miayn varchapetiny (Not only of the Prime Minister, in Armenian). Retrieved May 4, 2023 from: https://armeniasputnik.am/society/20200714/23724247/Voch-miayn-varchapetiny-HH-um-petakan-vor-karuycneri-kayqern-en-kotrel-adrbejancinery.html