Alizada C. Sh., Aliyev B. A.♦

DOI: 10.25108/2304-1730-1749.iolr.2018.55.21-37

Cyber security is an integral part of state security

Abstract: One of the most troubling issues in the globalization era is the issue of security and its provision.It is now possible to note that cyber security is becoming a strategic national issue that affects all levels of government and society.

In recent years, information and communication technologies (ICTs) develop so rapidly that it is often impossible to predetermine its subsequent consequences, and it is necessary to spend enough time, knowledge and knowledge to overcome the resulting negative situation. Basically, the new technologies, projects and programs that are used in the Internet global network seem to be beneficial and harmless at first, but experience shows that in many cases, it is impossible to get them completely.

The expansion of computer networks promotes the broader use of network technology capabilities in cyberspace, and enhances coordination, coverage and complexity in networking activities.This leads to the multiplication of cybercrime, by the users who are equipped with more advanced and modern ICT tools.

Based on the above, we can say that ensuring cyber security is a vital issue. A national policy on this issue and a cyber security strategy that is developed within this policy is required. As cyber attacks are likely to result in tangible and even possible consequences, cyber security is of great importance in determining

♦**Alizada Cavid Shirzad oglu** – Researcher of "The legal provision of state security" of the Institute on Law and Human Rights of the Azerbaijan National Academy of Sciences (Azerbaijan). E-mail:cavid6455@mail.ru

Aliyev Bakhtiyar Abdurahmanoglu – PhD in Law, Associate Professor, Head of the Department of "The legal provision of state security" Institute on Law and Human Rights of the Azerbaijan National Academy of Sciences (Azerbaijan). E-mail: antiterror-baku@mail.ru

and punishing those results and actions and methods that result in these consequences.

Keywords: cyber security; international cyber security strategies; cyber defense.

The concept of cyber security and its concepts are rapidly evolving recently and continue to evolve.In parallel with the development of information and information technologies, the concepts in this field are also rapidly multiplying dynamically. Cyber security was first used by computer engineers in the 1990s to describe security issues with network-connected computers, but when it became apparent that security problems could have devastating social consequences, it was estimated by influential people and the media as a major threat to the western world over time, electronic cyberplane ports.The terrorist act on September 11, 2001 in the United States, has focused on information technology and computer security, particularly in the protection of information technology infrastructure, electronic observation, and the use of terrorists as a means of communication in the Internet.The main threats to cyber security, threatening networks are relatively different.As such, threats to cyber security of states can be divided into two categories of cybercrime and external threats that threaten states' cyber security against each other. Cyber-clashes, economic espionage, and intelligence threats refer to the first category. Cybercrime crimes and cyber-terrorism are second-class threats [4].

It can be noted that the complex and multi-dimensional environment of cyber space has made cyber security one of the priority security areas.Cyber security as a means of protecting all types of information in the cyber environment, including the production and maintenance of data. In the broadest sense, cyber security is commonly used to protect the organization, organization and users of cyber media, security concepts, education, and technology [6].There are some

security criteria in the cyber environment. These should be privacy, integrity, integrity, consistency, reliability, durability [1]. Dissemination of secret information as a result of attacks on information systems, chaos can lead states to a difficult situation.

For example, a cyber-attack in Estonia in 2007 showed how important a country's infrastructure might be in the face of threats from the Internet.The reason for this threat in Estonia is the fact that it is through the Internet that many public and private sectors are involved in the Internet [2]. Again, in Australia, an abusive employee's manipulation of computer systems, the waste water, the programs that led to the deaths of 11 people in the US and the loss of 50 million lives in the United States, and the Stuxnet attacks on Iran's nuclear facilities among the examples.

The security of the layers of cyber security can be noted as security, service security and infrastructure security. Unver M. categorized cadmium classification in the form of detection, damage, deletion, disclosure, and discrimination [7]. Based on all this, almost all the work in the field of security requires a national policy and a cyber security strategy developed within this policy. As cyber attacks can have consequences that can affect even the most trivial and trivial issues, it is important that cybercrime be identified and punished as a criminal offense and the resulting actions and methods.In parallel with the development of technology, there is a need to review the country's legislation, taking into account the changing cyber-attacks and methods. Creating a legitimate framework on this issue is also an important issue, as the deficiencies should be eliminated.In addition to developing technical measures to improve the quality of software, hardware and business processes, as well as establishing an organization for providing cyber security, ensuring and developing international co-operation and coordination, as an important element in ensuring cyber security.

At present, there are states where there is no safe cyber environment. Assistance to such states is of particular importance. This, in turn, requires the development of cyberspace security strategies.

The activities of the EU (European Union) agencies on cyberpass security are concentrated in three major areas:

• development of the normative-legal base;

• establishment of institutional structures;

• implement information and educational campaigns among civil servants and members of the organization.

At present, the EU has created minimal necessary regulatory and legal framework for cyber-security issues. For example, in 2012, the European Commission worked out an "Internet Security Strategy" for the EU. The project aims at identifying economic and geopolitical opportunities along with key risks and challenges, comparing the level of preparedness for the Internet security problem in third countries, identifying the major problems required for solving and evaluating current and planned activities.

Strengthening the EU's capacity to fight cybercrime has been entrusted to the European Network and Information Security Agency (ENISA), established in September 2005.

Since January 1, 2013, the European Center for Cyber Security has been functioning within EuroPol, whose main goal is to improve the protection of citizens of EU member states from emerging cybercrime.

In October 2012, ENISA has launched a pilot project entitled "European Cyber Security Monthly" in order to improve the level of information on the cyber threats of the EU member states. The project envisaged conducting relevant advertising campaigns on television and radio, social networks, organizing conferences and round tables in several countries.

While developing a regulatory legal framework for cyber security and developing institutional structures, it is not enough for EU member states to prepare for the fight against potential cybercrime. This is particularly highlighted in the resolution of the European Parliament on November 22, 2012, titled "Resolution on cyber security and defense" [6]. The document highlights the danger of terrorist organizations' use of virtual spaces.It is reported that they have the potential to make cyber attacks critical for the EU.

In order to eliminate these shortcomings, the European Commission has issued a "European Union Cyber Security Strategy: Open, Reliable and Safe Cyberpace" on 07 February 2013.The strategy provides clear priorities for the EU's international cyber security policy:

• Freedom and clarity: This strategy defines views and principles in the application of core EU values and fundamental rights in cyberpower.

• Laws, norms and key EU values are applied at the same level as in the physical world: the responsibility for safer cyberfighting lies with all the participants of global information society from states to states.

•Building a cyber security potential: The EU will work with international partners and organizations, the private sector, and civil society to support the global capacity building in third countries. This will include information access and improved access to the open Internet and cyber threats.

• Developing international cooperation in cyber security issues: Keeping open, free and safe cyberfighting is a global challenge and the EU will seek to resolve this problem with relevant international partners and organizations, the private sector, and civil society.

The key provisions of the strategy are:

• Developing national cyber security strategies by all EU Member States;

• mandatory ratification by the European Union's Cybercrime Convention as a major international instrument for combating crime in cyberspace by all participants of a political organization;

• the application of a single list of standards for the preparation of countries to combat cybercrime;

• Absolutely informing the European authorities of certain national authorities about the identified cyberpatients;

• Improving co-operation between civilian and defense sectors in cybersecurity.

The European Union's cyber security strategy came into force on June 19, 2013, and according to this document, the powers of ENISA extended to seven years. EU governments are instructed to establish anti-cyber security bodies, finance, transport and energy companies - cybercrime measures.As in the US strategy, the creators of the EU program also rely on cooperation between private and public sectors.

NATO decided to set up security centers for cybercrime and cyber security in Bucharest summit in 2008 after mass cyber attacks on the Estonian network system in 2007.At the meeting, it was stated that ensuring the security of cyber security is, first and foremost, the duty of the states.However, the cyber threats from NATO's 2010 summit in Lisbon have been included in the list of threats targeting NATO nations after the proliferation of weapons of mass destruction and terrorism.NATO has already developed documents such as the "Cyber Defense Policy" and the "Cyber Defense Concept". However, these documents are confidential and only the summary information about them can be found on the official website of the alliance. Members of the alliance in defining principles of cyberspace define principles of allied solidarity and recognition of national sovereignty. In other words, the overall objective is that all NATO allies should be ready for cyber attacks and have the potential to support each other during such

attacks.In order to achieve this goal, allies should develop their cyber-defense capabilities within their own countries. In this context, bilateral and multilateral close cooperation networks are established under the umbrella of NATO.

Elements for the establishment of a global cyber security culture have been approved by Resolution 57/239 of the General Assembly of the United Nations (UN) of 20 December 2002.

At present, the dependence on Azerbaijan's computer infrastructure is rising. Attacks on computer systems so far have been hackers' world-class computer viruses, yet existing cyber-threatening threats can be expanding and worrying in the future. It is difficult to maintain the safety of technology systems. If Azerbaijan's formal and informal technology infrastructure does not become safer, it can cause serious consequences in the future.

References

1. Gorman, Sean P. (2006). A Cyber Threat to National Security? (Edited By: Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan). Seeds of Disaster, Roots of Response. Cambridge: Cambridge University Press, 239-257.

2. Lewis J.A. Assessing the risks of cyber terrorism, cyber war and other cyber threats // Center for Strategic and International Studies, 2002, pp. 3-12. Alekperova IY Information war technology, publishing house "Information Technologies", Baku, 2012, 108 p.

3. Nye, Joseph, Jr. (2011). Nuclear Lessons for Cyber Security? Strategic Studies Quarterly, Wınter-2011, 18-38.

4. Power, Ayhan (2015). An Assessment on Realistic Cyber Attacks Against Critical Energy Infrastructure. (Editor: Mesut Hakkı Caşin). International Critical

Energy Infrastructure Security: New Threats and Opportunities. Caspian Strategy Institute, pp.18-39

5. Sawyer P. Tret'ya mirovaya voyina mozhet nachat'sya v internete [Third world war can begin in Internet]// Computerworld Russia, Moscow, № 32, 2009, p. 29, Alakbarova I.Y. Information war technology, publishing house "Information Technologies", Baku, 2012, 108 p.

6. Stevens, Tim (2015). Cyber Security, Community, Time, Cyber Security and the Politics of Time. Cambridge: Cambridge University Press.

7. Unver Mustafa and Canbay Cafer. (2010). "National and International Dimensions of Cyber Security", Journal of Electrical Engineering, Issue 438.