DOI 10.18372/2786-5495.1.17309

Zahid Oruj,

Chairman of the Board of the Social Research Center,

Baku, Azerbaijan

zahidoruc@gmail.com

CYBER SECURITY: CONTEMPORARY CYBER THREATS AND NATIONAL STRATEGIES

Annotation. *The article is devoted to the study of the basic strategies and doctrines of cyber security and cyber threats. Cyber-attacks have become as commonplace as the Internet itself. Each year, industry reports, media outlets and academic articles highlight this increased prevalence, spanning both the amount and variety of attacks and cybercrimes. It is noted that today information security and cyber security in official documents -concepts, doctrines, charters-of many countries are considered to a large extent as independent concepts that are not related (or very slightly related) to each other, and information security and cyber security are considered as independent areas of activity, little intersecting with each other. This artificial division is due to the fact that in the special services of these countries, information security is mainly carried out by operational agents, whose main tool is operational combinations on the channels of open telecommunication networks and cybersecurity is carried out by technical and operational-technical workers (including hacker programmers, hardware specialists, etc.), whose main form of activity is cyberattacks on the protected information resources of the enemy. Purpose of the research: improvement of the scientific and methodological theoretical and legal foundations of cyber security. Research method: a comprehensive theoretical and comparative analysis of the current legislation of foreign countries and Azerbaijan in conjunction with an analysis of law enforcement practice. Results: the features of the legal regulation of cyber security in Russian*

and foreign legislation are shown, highlighted the main properties of the concept of cybersecurity.

Анотація. *Стаття присвячена дослідженню основних стратегій і доктрин кібербезпеки та кіберзагроз. Кібератаки стали таким же звичним явищем, як і сам Інтернет. Щороку галузеві звіти, засоби масової інформації та академічні статті підкреслюють ще збільшення поширеності, охоплюючи як кількість, так і різноманітність атак та кіберзлочинів. Зазначається, що сьогодні інформаційна безпека та кібербезпека в офіційних документах – концепціях, доктринах, хартіях – багатьох країн розглядаються, значною мірою, як самостійні поняття, які не пов'язані (або дуже незначно) одна з одною, а інформаційна безпека та кібербезпека розглядаються як самостійні сфери діяльності, мало перетинаються між собою. Такий штучний поділ пов'язаний з тим, що в спецслужбах цих країн інформаційна безпека в основному здійснюється оперативними агентами, основним інструментом яких є оперативні комбінації на каналах відкритих телекомунікаційних мереж, а кібербезпека здійснюється технічними та оперативними засобами, технічніми працівниками (у тому числі хакери-програмісти, апаратники тощо), основною формою діяльності яких є кібератаки на захищені інформаційні ресурси противника. Мета дослідження: удосконалення науково-методологічних теоретико-правових засад кібербезпеки. Метод дослідження: комплексний теоретичний і порівняльний аналіз чинного законодавства зарубіжних країн та Азербайджану в поєднанні з аналізом правозастосовчої практики. Результати: показано особливості правового регулювання кібербезпеки в російському та зарубіжному законодавстві, виділено основні властивості поняття кібербезпека.*

Key words: *cybercrime, cybersecurity, national strategy, cyber-attacks, information protection, digital technologies principles information and communication technologies (İCT)*

Ключові слова: *кіберзлочинність, кібербезпека, національна стратегія, кібератаки, захист інформації, цифрові технології, принципи інформаційно-комунікаційних технологій (ІСТ)*

The modern global strategy of world social development is determined by the general idea of digital transformation of all spheres of everyday life. Under these conditions, cybersecurity issues are of particular relevance as a response to the modern «digital revolution», which finds its expression in the creation and rapid development of modern digital, information and communication technologies, their widespread use in various fields of activity, and, as a result, in the formation of «digital» economy, «digitalization» of the system of law.

Modern digital and IT technologies, including, in particular: the Internet of Things (Internet of Things), artificial intelligence and modern robotics (AI & robotics), big data (Big data) and analytics, cloud computing (Cloud computing), digital modeling and augmented reality (augmented reality & simulation), additive manufacturing (additive manufacturing) - in their totality and interconnection create the technological foundation of the «digital economy», new social and public relations in the virtual digital space. In modern conditions, in order to increase capitalization and obtain competitive business advantages, new digital industrial technologies are used, which are defined by the term «Industry 4.0» and form a new fourth world technological revolution - the "digital revolution". are the driving force behind overall growth [1].

Digital technologies have a strong impact on governance structures, including public administrations. The formation of cyberspace and the use of new technologies in it based on the basic principle of a distributed (decentralized) registry (blockchain tech) led to the creation of a fundamentally new toolkit: smart contracts, digital signatures, basic technological patents, standards and rules, etc.

The European Union Agency for Network And Information Security (ENISA) 2018 report9 notes that the threats and risks associated with IoT devices, systems

and services are diverse and rapidly evolving. The Internet of Things has an increasing impact on the security and privacy of citizens, and the types of threats against the Internet of Things are extremely diverse [2].

In order to manage and mitigate the risks associated with virtual assets, countries are encouraged to regulate the provision of services with virtual assets on the basis of licensing or registration of such services and subject them to effective monitoring systems and compliance with FATF recommendations.

The path of digital transformation requires a fundamental restructuring of the approaches of private business and the state to interaction, decision-making, stimulating innovation and the formation, including the digitalization of the legal system, where each participant in the system has its own significant role. Governments of developed countries worked out ambitious programs to create and improve digital services for various public services and even entire areas of society.

Definitions and Meanings

*Cybersecurity i*s a practice of protecting systems, computers, networks, programs, personal data, etc., from unauthorized access, digital attacks and threats. It is an activity by which information and other communication systems are protected and defended against the unauthorized use or modification or exploitation of the device. Cybersecurity is also called information technology security. It includes the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that can cause damage to them or exploit them in any way. Basically, cybersecurity is a technical approach to secure systems from such attacks.

Regarding the definition of the term *cyber strategy:* the cybersecurity strategy is a document that fixes the state policy aimed at ensuring the security of the state in cyberspace.

There are various definitions of the term «cybersecurity», formulated at the national and international levels. For the purposes of this document, the following meaning of the term «cybersecurity» is used: it is a set of tools, strategies,

guidelines, risk management approaches, actions, training, best practices, safeguards and technologies that can be used to protect the availability, integrity and confidentiality of resources. in connected infrastructure used by government agencies, private organizations and citizens; such resources include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and data in a cyber environment.

In 2015, the European Network and Information Security Agency (ENISA) released the document «Defining cybersecurity: gaps and overlaps in standardization», which provides definitions of the concept of «cybersecurity» in various international standards and documents [3].

Organizations across industries use (if they use) their own definition of «cybersecurity». For example, in the media, this concept is used in relation to everything that can disrupt the operation of a computer, and it means «threat to cybersecurity». Military organizations or the state apparatus approach «cybersecurity» from a strategic point of view. They also use the term «cyber security» in conjunction with the term «cyber warfare». Figure 1 illustrates the different domains within the term «Cybersecurity».

Figure 1: Different domains of Cybersecurity

Fug. 1. The different domains within the term «Cybersecurity»*
*Sourse: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [4]

In language terms «Cybersecurity» or «cyber security», depending on the organization and the spelling of the word within its context, is a rather young term. Originated on the term «Cyber Space», the term «Cybersecurity» was crafted and

used by IT professionals, consultants, lobbyists and politics to address security concerns in the «Cyber Space». But what does this mean? Does «Cybersecurity» only address risks originating in the «Cyber Space»? Does «Cyber security» only consider the protection of virtual assets within the «Cyber Space»? Does «Cyber security» also apply to physical assets, such as Industrial Control Systems, production lines, power plants, etc. although they are not primarily designed to be in the «Cyberspace»?

The article explores the cybersecurity strategies of the most active states on the world stage, considers individual units that specialize in conducting not only defensive, but also offensive operations in cyberspace, analyzed the goals of creating departments responsible for cyber operations. The choice is determined by the level of representation of countries in cyberspace - these are countries in relation to which the concepts of «cyberpower» or «cyberweapon» are most often mentioned, of which, first of all, those countries are considered in which documents on the topic under study are in the public domain. For example, while the DPRK is often featured in the media as a state that sponsors hacker groups and has the potential for cyber offensives, there are no documents in the public domain regarding the cybersecurity or cyber operations of this state (excerpts from the media will be included in the report)

There is following levels of cybersecurity strategies exist: State alliance strategies, like those of the EU and NATO (the NATO bloc does not have an official cybersecurity strategy, but in fact it is the «Tallinn Guide to International Law Applicable to Cyber Warfare», despite the fact that it is positioned as the opinion of an international group of experts); State (national) strategies; Industry Strategies: Peaceful industries, for example, the United Kingdom Civil Nuclear Safety Strategy, etc.

Information and communication technologies (ICT) are rapidly developing, increasing their influence on all key areas of activity of a citizen, organizations and the state in the different countries. The Internet and other components of cyberspace

have established themselves as a system-forming factor in every states economic development and modernization. The introduction of ICT in the processes of public administration is the basis for building an effective and socially responsible democratic state in the 21st century. In this regard, a targeted and systematic state policy for the development of the national sector of information technology application is required.

At the same time, along with a significant increase in opportunities, the penetration of ICT into all spheres of life causes the emergence of a number of new and the development of some existing threats to the individual, society and the state. The cross-border nature of cyberspace, its dependence on complex information technologies, the active use of cyberspace platforms and services by all groups of Russian citizens define new opportunities, but at the same time develop new threats for: damaging the rights, interests and life of an individual, organization, state bodies; conducting cyberattacks against protected information resources by cybercriminals and cyberterrorists; the use of cyber weapons in the framework of special operations and cyber wars, including those accompanying traditional military operations.

An Overview of Some National Cybersecurity Strategies

At the present stage, cybersecurity is turning into a strategic national problem that affects all levels of society. «A flexible, agile and effective response to cyber threats requires the correct definition of national goals and priorities achieved over a certain period of time, as well as the roles and responsibilities of stakeholders. National cybersecurity strategies are the first step in this direction. In order to identify best practices in the development of national cybersecurity strategies, this paper analyzes existing national cybersecurity strategies» [5].

Currently, a number of countries have adopted a number of documents aimed at ensuring various aspects of national information security. Among them are the Doctrine of Information Security, the Strategy for the Development of the Information Society and other documents. However, the existing regulation does not

adequately cover the system of relations that arise within the framework of cyberspace as an element of the information space. In order to implement the opportunities associated with the use of the cyberspace functionality and establish control over emerging risks, the question arises of the need to prepare a special document in this area. Taking into account the complex nature of the problem, its scale, the prospect of long-term development, accumulated international experience, it seems reasonable to choose a strategy as a form of document.

Cybersecurity and the Strategy Development Process National cybersecurity strategies can take many forms and differ in different levels of detail, depending on the goals and level of preparedness for cyber threats of each particular country. Accordingly, there is no established and generally accepted definition of the elements that make up a national cybersecurity strategy.

Research recommends that a national cybersecurity strategy be viewed as:

– an expression of the high-level vision, goals, principles and priorities that guide a country in cybersecurity;

– an overview of the stakeholders charged with strengthening the country's cybersecurity and their respective roles and responsibilities;

– a description of the measures, programs and initiatives that the country will implement to protect its national cyber infrastructure and at the same time strengthen its security and resilience.

Given that society is becoming more dependent on information and communication technologies every day, the protection and availability of these technologies is becoming a critical moment and a very important topic for national interests. Today, a necessary condition for the development of the information society is cybersecurity, behind which there can be an almost endless list of security problems and their solutions, ranging from technical to legislative. In modern conditions, cybersecurity issues go from the level of information protection at a separate computer facility to the level of creating a unified cybersecurity system as an integral part of the information and national security of each state.

On the world stage, the information security policy in a particular state is ensured through the adoption of Cybersecurity Strategies. So, the first cybersecurity strategy appeared in 2003 in the *United States of America*. (September 2018 Natıonal Cyber Strategy of the United States of America 2018). After that, similar Strategies and action plans for security in the virtual space spread throughout Europe.

According to the Competitiveness Index-2016, published by the IMD World Competitiveness Center, Israel is the leader in cybersecurity out of 61 countries. As the most computerized country in the Middle East, Israel has created an information security department under the General Security Service (SHABAK) that controls critical national infrastructures, including electricity generation, water supply, and so on. The *Israel* International Cyber Strategy serves as a compass for Israeli international engagement on cybersecurity. It outlines Israel's main positions on international cybersecurity issues and serves as a platform for discussion and coordination with partners [6].

İn 2022 The Biden administration has released a new USA National Security Strategy that, like many strategies, addresses the country's cybersecurity issues. Let's take a quick look at the main provisions of the document and what exactly it refers to cybersecurity. The new version of the strategy was published on October 12, 2022 [7].

The main goals are proclaimed: the security of the American people, the expansion of economic opportunities and the protection of democratic values.

To achieve these goals, the United States intends to:

– Invest in the tools and leverage of American influence.

– Create the strongest possible coalition of states for collective influence in order to form a global strategic space.

– Modernize and strengthen the army to be ready for the era of strategic rivalry.

The new US national security strategy takes into account the current geopolitical situation, and among the mentions of other countries, the most attention is paid to Russia. Russia is called «a source of instability on a global scale», a danger and a threat that must be contained, and China is recognized as the only competitor to the United States and a «serious geopolitical challenge».

Awareness of the growing cyber threats, both in the military and in the civilian field, led to the decision to create an ad hoc group of almost a hundred specialists, which a year later presented recommendations for relative innovations at the national level in order to prepare for future cyber war threats. Innovations concerned not only the development of specific technologies, but also the creation of the necessary infrastructure, including the cooperation of industrial and academic circles with national security structures, educational programs within the school system of education, the creation of academic centers of excellence, critical national systems and many other projects.

Published in 2010, *Canada's* national cybersecurity strategy rests on three pillars:

– Protection of government systems.

– Collaborate to protect key cyber systems outside of the federal government.

– Keeping Canadian citizens safe online.

The first pillar involves establishing clear roles and responsibilities, strengthening the security of federal cyber systems, and raising government cybersecurity awareness.

The second «pillar» is a series of state-level partnership projects involving the private sector and the critical infrastructure sectors.

And finally, the third «pillar» is the fight against cybercrime and the protection of Canadian citizens in the online environment. There is also the issue of personal data [8].

In 2011, the *Israeli* National Cybersecurity Bureau was established to oversee, plan and implement these innovations. As this problem became more and more

urgent on a global scale, the experience gained in Israel and the corresponding government strategy gradually turned individual private companies into a powerful sector of the country's economy. Today, Israel's cybersecurity infrastructure includes about 150 companies, including established firms like Check Point, and startups, venture capital funds that invest in this particular area, like Jerusalem Venture Partners (JVP) Cyber Labs, as well as research and development projects. implementing cooperation between high-tech companies and academia.

The Netherlands, cybersecurity strategy (2011) on the one hand, strives for safe and reliable information and communication systems, fearing serious violations in these systems, and on the other hand, recognizes the need for a free and open Internet space. The strategy defines cybersecurity. «Cyber security is protection against failures and misuse of information and telecommunication systems. Failures and misuse can adversely affect the availability and reliability of information and telecommunications systems, jeopardize the confidentiality and integrity of information stored in systems» [9].

Japan's Cyber Security Strategy12 (May 2010) can also be subdivided into several key areas of action:

- Strengthening policies aimed at combating possible massive cyber-attacks and establishing a body responsible for preventing attacks;

- The introduction of policies that easily adapt to changes in the field of information security;

- Preference of active information security policies to passive ones.

The *United Kingdom's* National Cybersecurity Strategy (2011) approach also aims to advance cybersecurity. Goal: To bring the United Kingdom to the forefront of innovation, investment and quality of service in information and telecommunications technology, and thereby take full advantage of all the benefits and virtues of cyberspace. It is necessary to exclude risks such as cyberattacks by criminals, terrorists and other states in order to make cyberspace safe for citizens and the economy [10].

A list of all national Cybersecurity Strategies of the *European Union* (EU) countries and some other non-member countries is published by The European Network and Information Security Agency (ENISA). The *German* Cybersecurity Strategy was adopted in early 2011, with the German Strategy focusing on preventing and prosecuting cyberattacks and preventing failure of IT equipment that could be caused by random factors [11].

Also, the German Strategy analyzes the need for additional actions to protect IT systems through the provision of basic state-certified security functions, as well as support for small and medium-sized businesses through the creation of a new working group. In addition, on July 11, 2015, the German Parliament adopted a law on cybersecurity, according to which more than 2,000 service providers will be forced to introduce new security standards in cyberspace within two years; otherwise German companies face a fine of 100 thousand euros. The law affects institutions listed as «critical infrastructure» such as transportation, healthcare, water utilities, telecommunications providers, and financial and insurance companies. At the same time, the new law obliges companies to report any cyberattacks to the German Federal Office for Information Security (BSI).

Another example from the EU countries is Estonia. This cybersecurity strategy for 2019-2022 is Estonia's third national cybersecurity strategy document and defines the long-term vision, objectives, priority action areas, roles and tasks for the domain, being the basis for activity planning and resource allocation [12].

National Cyber Security Strategy *France* (2011) focuses on ensuring that information systems are able to withstand events in cyberspace that can adversely affect the availability, integrity and confidentiality of information. France is focusing on technical means of protecting information, combating cybercrime and establishing cyber defenses [13].

Cyber Security Strategy of *Estonia* for 2014-2017 was adopted and is the main cyber security planning document, continuing the implementation of many of the goals found in the Cyber Security Strategy 2008-2013. The four-year goal of the

cybersecurity strategy is to increase cybersecurity capacity and increase public awareness of cyber threats, thus creating confidence in cyberspace, including ensuring the protection of information systems underlying life support services, overcoming cyber threats to the public and private sectors, implementing a national system control in the field of cybersecurity, ensuring the integrity of the digital resources of the state, promoting international cooperation in the field of protecting the infrastructure of critical information, improving the fight against cybercrime, raising public awareness of cyber risks, developing a legislative framework for ensuring cybersecurity, and others. In addition, on May 4, 2008, at the meeting of the NATO Council in Brussels, a Memorandum of Understanding was signed on the establishment of a NATO cyber defense center in Tallinn, later called the NATO cooperative cyber defense center of excellence [14].

At the heart of *Finland's* strategy is the understanding of cybersecurity (2008) as an economic issue closely linked to the development of the Finnish information society.

The Concept of the Cybersecurity Strategy of the Russian Federation substantiates the necessity and timeliness of the development of the Cybersecurity Strategy of the Russian Federation (hereinafter referred to as the Strategy), determines its principles and directions, as well as its place in the system of state regulations [15].

As in many countries, developing a national cyber cybersecurity policy is essential for *Azerbaijan* as well. Government information and communication systems, as well as military and commercial projects, are becoming more vulnerable to cyberattacks and cyber espionage. From this perspective, it becomes crucial to manage the cyber space of a country at the state level. Azerbaijani authorities are very active in prioritizing cyber-security in their policies.

Cybersecurity legal and regulatory frameworks (laws, doctrines, and improvements to existing legislation) establish the legal and organizational framework for ensuring the cybersecurity of the state, directions, and principles of

state policy in the field of cybersecurity. And also the powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this sphere and the basic principles of coordination of their activities. Development of legal and regulatory frameworks of cybersecurity policy of Azerbaijan mainly started in the 1999-2000s [16].

Apart from legal documents that are related to cybersecurity, some policies directly concern cybersecurity. It is important to mention that there is no separate strategy on cybersecurity or cooperation with the private sector on the issue, but there are some provisions in various policies that are related to developing cybersecurity capabilities. These strategies are «National Strategy on the Development of Information Society for 2014-2020» and «2016-2020 State Program on the Implementation of the National Strategy for the Development of Information Society», «Azerbaijan 2020: Concept of Development», and «Strategic Road Map for the Development of Communication and Information Technologies».

«The National Strategy for Development of Information Society in Azerbaijan during 2014- 2020» takes into account all experiences and recommendations which have been made by ITU and the EU. The strategy's main goal is to «build an information society and make efficient use of its capabilities by citizens, communities, and the state for the country's sustainable socioeconomic, cultural, and economic development, including the development of ICT».

Currently the new National Strategy of Azerbaijan in the field of cyber security and information is being developed by a number of departments and organizations, including the Ministry of Digital Development and Transport, the State Electronic Protection Service, the State Security Service and a number of other structures. All issues related to cybersecurity will be included in this document. The adoption of this document is very important in terms of increasing the rating of Azerbaijan in the field of cybersecurity. In 2020, Azerbaijan has risen by 15 positions in the cybersecurity rating. But the rating is reviewed every two years, and here it is important that this strategy be adopted in order to achieve even better results.

Conclusion. As can be seen, world experience shows that today cybersecurity issues are of a global nature, which in turn necessitates the development of not only a national, but also an appropriate international security strategy. It is quite obvious that in the modern world, in which cyberspace and modern information technologies play an increasingly important role in the life of the state, its economy and security system, one cannot ignore the threats associated with the use of high technologies. Here the Republic of Azerbaijan is no exception, the high pace of development of information and communication technologies in Azerbaijan actualizes the protection of the relevant infrastructure, since its damage or destruction can have significant consequences for the country's security.

Countries have different views on cybersecurity, there are views on cybersecurity as an information security problem, a national security problem, a law enforcement problem, and an economic problem. Although all countries recognize the importance of international cooperation in the field of cybersecurity, the lack of a common «language» and approach makes international cooperation difficult. Therefore, countries need to agree on a generally accepted definition of the term cybersecurity. Reliable cybersecurity goes beyond the capabilities of the state alone, the solution of this task requires partnership and cooperation of all interested parties - the state, the private sector and citizens. The cross-border nature of cyber threats encourages countries to work closely together on cyber security. It should also be analyzed whether the cybersecurity strategy is consistent with the goals of the international community and whether it supports the fight against cybersecurity issues at the global level.

References

1. Digitalization for All Future-Oriented Policies for a Globally Connected World.G20, 2017. URL: https://www.b20germany.org/filead-min/user_upload/documents/B20/ B20Digitalization_ Policy_Paper_2017.pdf; OECD Digital Economy Outlook 2017. OECD, 2017. URL:

https://doi.org/10.1787/cc76d818/; Networks of «Things». NIST Special Publication 800-183. U.S. Department of Commerce, July 2016. URL: https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP. 800-183.pdf

2. Baseline Security Recommendations for loT in the context of Critical Information Infrastructures. European Union Agency For Network And Information Security, November 2017. URL: www.enisa.europa.eu. P.11-12, 19.

3. Definition of Cybersecurity. Gaps and overlaps in standardization. V1.0.December 2015. URL: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

4. Yadigar N. Imamverdiyev. Next Generation National Cyber Security Strategies. *Problems of Information Society.İnformation Technology Publishing House* . 2013, № 2(8), P. 42-51

5. Israel International Cyber Strategy. *International Engagement for Global Resilience*. July. 2021. URL: https://www.gov.il/BlobFolder/news/international_strategy/en/Israel%20International%20Cyber%20Strategy.pdf

6. National Security Strategy. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

7. http://publications.gc.ca/site/eng/379746/publication.html

8. http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

9. http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

10. Cyber Security Strategy for Germany 2016. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Germany_2011_Cyber_Security_Strategy_for_Germany.pdf

11. Government Cyber Security Strategy. URL: https://e-estonia.com/programme/cyber-security/#:~:text=This%20cybersecurity%20strategy%20for%202019,activity%20planning%20and%20resource%20allocation

12. http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

13. http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

14. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

15. https://report.az/ru/ikt/rahid-alekberli-stroitelstvo-umnogo-sela-i-umnogo-goroda-sozdaet-osnovu-dlya-formirovaniya-kiber-sredy/

16. İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı. 26 sentyabr 2012-ci il.

17. Luijf H., Besseling K., Spoelstra M., de Graaf P., Ten national cyber security strategies: a comparison. *Proc. 6th International Conference on Critical Information Infrastructures Security (CRITIS 2011),* September, 2011.

18. The ITU National cybersecurity strategy guide. Geneva, 2012, 122 p.

.