Studia Bezpieczeństwa Narodowego
Zeszyt 23 (2022)
ISSN 1508-5430, s. 19-26
DOI: 10.37055/sbn/149510

Instytut Bezpieczeństwa i Obronności
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 23 (2022)
ISSN 1508-5430, pp. 19-26
DOI: 10.37055/sbn/149510

Institute of Security and Defense
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

THE STATE OF THE CYBER ENVIRONMENT AND NATIONAL CYBERSECURITY STRATEGY IN DEVELOPED COUNTRIES

STAN ŚRODOWISKA CYBERNETYCZNEGO I NARODOWA STRATEGIA CYBERBEZPIECZEŃSTWA W KRAJACH ROZWINIĘTYCH

Elshan Tanriverdiyev
elshan.tanriverdiyev@gmail.com
The War College of the Armed Forces

Abstract. The article analyzes the state of cybersecurity in developed countries, the strategies available in this area, and identifies their common and distinctive features in order to study advanced practices in developing and improving a national cybersecurity strategy. The aim of the article is to analyze and compare the national cybersecurity strategies of developed countries. The methods of examining source documents and statistical analysis were used.
Keywords: information security, information war, cybersecurity, cyber environment, cybersecurity strategy, cyberattack
Abstrakt. W artykule przeprowadzono analizę stanu cyberbezpieczeństwa w krajach rozwiniętych, przedstawiono strategie dostępne w tym obszarze oraz ich wspólne i wyróżniające cechy w celu zbadania zaawansowanych praktyk w zakresie opracowywania i doskonalenia krajowej strategii cyberbezpieczeństwa. Celem artykułu jest analiza i porównanie narodowych strategii cyberbezpieczeństwa krajów rozwiniętych. Zastosowano metody: badania dokumentów źródłowych oraz analizy statystycznej.
Słowa kluczowe: bezpieczeństwo informacji, wojna informacyjna, cyberbezpieczeństwo, cyberprzestrzeń, strategia cyberbezpieczeństwa, cyberatak

Introduction

In the context of integration into modern information technologies, the state, society, business structures and individuals face critical challenges in the field of information and its authenticity in cyberspace, secure use of electronic services, protection of personal data, data completeness and confidentiality. In an environment where new cyber threats are constantly emerging and evolving, it is important for countries to have flexible, operational cybersecurity strategies against global cyber threats.

In the modern era, cyberattacks and cyber defense are considered as an integral part of all operations. At present, no military operation is carried out without a cyber element. However, very few countries are able to respond to such attacks with state resources (Hasanov, 2016, p. 112-115).

Today, the issue of cybersecurity is considered one of the priorities. Every year, governmental, non-governmental and international organizations hold various events in this area at the regional and global levels. As it is seen, cybersecurity is a very broad and urgent problem. The Azerbaijani state has taken appropriate steps to assess the existing gaps and threats in this area in a timely manner and will continue to work with great determination (Hasanov, Iskandarov, 2017, p. 60-67).

Significant changes have taken place in the organization of cyberattacks on the information infrastructure of organizations. It is known as Advanced Persistent Threat (APT).

The difference between APT and traditional types of cyberattacks is a well-organized project approach, planning, financing and sustainability. Such attacks can last for months or even years, depending on the issues facing the executors. In many cases, the goal is not to destroy the network or to deal a crushing blow to it, but to obtain, analyze, and use information for a long period of time (Imamverdiyev, 2013, p. 14-17).

Currently, the number of cyberattacks and cyber-espionage against government agencies and private companies is growing rapidly. The consequences of well-planned and successful cyberattacks targeting interconnected and dependent information infrastructure can be devastating. Cybersecurity and privacy of personal information is becoming a strategic national issue affecting all levels of society. Therefore, cybersecurity becomes a necessary condition for the development of the information society (Sood, Enbody, 2013, p. 54-61).

Cybersecurity strategies of developed countries

The United States is the first country to recognize cybersecurity as a key national strategic issue. The Critical Infrastructure Protection Document, adopted in 1998, set out key areas for action on critical infrastructure and information security. Following

the terrorist attacks in the United States on September 11, 2001, a detailed project was implemented to review the Internet security policy. As a result, in 2003, the "National Cybersecurity Strategy" was adopted. This strategy is part of the "National Security Strategy" adopted after the terrorist attack.

In 2018, the US Cyber Security Strategy was updated and the Comprehensive National Cybersecurity Initiative (CNCI) strategy was approved. CNCI consisted of 12 secret initiatives. Over time, some of its details were announced at conferences. CNCI envisioned several large-scale changes. The first required a reduction in network connections between federal agencies and foreign providers from 4,000 to 50 over a four-month period.

Second, the National Security Agency (ENSTEIN), a program that monitors Internet traffic from federal websites to other websites (developed by the United States Cyber Security Incident Response Team in 2004 to detect and block cyberattacks) Security Agency). In the new version of this program, in addition to federal networks such as traffic, content storage and monitoring, proactively private networks also have tracking features (US Government, 2009, p. 38).

CNCI also covered topics such as increasing investment in scientific and practical work in the field of cybersecurity, and promoting the sharing of information between government agencies.

In those years, Action Plans and strategies were adopted in Europe. In 2005, Germany adopted the "National Plan for the protection of Information Infrastructure". In 2007, Switzerland developed a strategy to improve Internet Security. Estonia in 2007 and Georgia in 2008 after a number of serious cyberattacks that paralyzed the information infrastructure, a number of NATO countries began to develop, adopt national cybersecurity strategies. Currently, more than 10 NATO member countries have adopted a national cybersecurity strategy, and some are developing similar national strategies (Luiijf et. al., 2011, p. 78-80).

In **Germany**, in February 2011, the "Cyber Security Strategy" was adopted and the National Cyber Defense Agency was established. The Agency cooperates with the Federal Office of Police, Intelligence and Information Security. As in the American strategy, there is a secret part in the German strategy. It is believed that this section is devoted to countermeasures against information attacks (Mitra, Schwartz, 2001).

Estonia became the first EU country to take such a step in 2008, adopting a comprehensive national cybersecurity strategy. The main directions of Estonia's national cybersecurity strategy are the strengthening of policies aimed at combating possible mass cyberattacks, the implementation of policies that are easily adapted to changes in the field of information security and the joint action of the authorities responsible for preventing attacks.

The goal of the **UK**'s cybersecurity strategy, which came into force in November 2011, is to make the country a leader in innovation, investment and service quality in the field of ICT, thus taking full advantage of the cyberspace. In order to make

cyberspace safer for citizens and the economy, it is intended to exclude risks such as criminals, terrorists and cyberattacks by other states (National Audit Office, 2013, p. 43).

France (2011) considers the ability of information systems to withstand events that could compromise the accessibility, completeness and confidentiality of data in cyberspace. The country considers it necessary to establish technical means for the security of information systems and a cyber defense system to combat cybercrime (ENISA, p. 15).

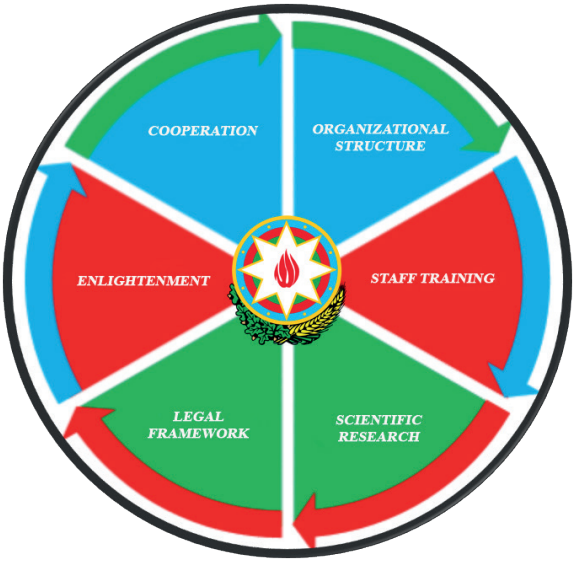
Canada's cybersecurity strategy, published in 2010, addresses three key areas: defining clear roles and responsibilities for the security of public systems, strengthening the security of federal cyber systems, and improving cybersecurity knowledge in government; a number of partnership initiatives in the regions involving the private and critical infrastructure sectors to ensure the cyber security of critical systems not owned by the federal government; combating cybercrime and protecting Canadian citizens online.

The Cybersecurity Strategy of the Republic of Poland is a document adopted by way of a resolution of the Council of Ministers, the document determines the strategic objectives, and the relevant political and regulatory measures directed at attaining and maintaining a high level of cybersecurity (Chałubińska-Jentkiewicz et. al., 2022, p. 114).

The purpose of this document is to define strategic objectives and relevant political and regulatory measures to achieve a high level of cybersecurity, principally a resilience to cyber threats of information systems used by operators of essential services, critical infrastructure operators, digital service providers and the public administration, as well as to increase information protection in the information systems by means of standardized safeguards. The achievement of the strategic objectives shall also contribute to increasing the national security, improving the effectiveness of law enforcement agencies and judicial authorities in detecting and combating cybercrime, events of a hybrid nature (including events of a terrorist nature) and cyberespionage. The Strategy takes into account, in particular : 1. cybersecurity objectives and priorities; 2. entities involved in the implementation and deployment of the Strategy; 3. measures used to achieve the objectives of the Strategy; 4. specification of means for readiness, response and restoration, including principles of public-private cooperation; 5. risk assessment approach; 6. activities related to educational, information and training programmes regarding cybersecurity; 7. activities related to research and development plans regarding cybersecurity (Ministry of Digital Affairs, 2019).

Turkey's "National Cyber Security Strategy and Action Plan for 2013-2014" was approved in June 2013. The Action Plan outlines the cyber risks and identifies 29 activities in 7 areas during the planned period through inter-agency cooperation (Resmi Gazete, 2013).

In general, each national cybersecurity strategy is required to be more effective and sustainable:



Picture.1. National Cybersecurity Strategy Model

Organizational structure. Cybersecurity strategies provide for the construction of an agile management model aimed at ensuring cybersecurity. In many countries, several government bodies and organizations consisting of various institutions bear responsibility for cybersecurity. This factor requires the integration of organizations with various cybersecurity goals and coordination roles into a single structure.

Legal framework. It is noted that there is a need to create a legislative base for the protection of cyberspace in some strategies. The legal and regulatory framework includes planning and defining the essential policies and regulatory mechanisms, clarifying the roles, rights and responsibilities of interested parties, basic measures and instructions for ensuring information security, new standards of logistics and etc.

Scientific research. It is necessary to conduct comprehensive scientific practical research aimed at solving the problems of security and sustainability of both existing and future systems and services. A number of strategies provide for the identification of a leading center for research and development in the field of cybersecurity and providing investments to eliminate the backlog.

Staff training. There is a need for new educational programs focused on the teaching of IT and cybersecurity specialists, as well as trainings that improve the users' skills. Some national strategies aim to improve the educational programs of information security specialists to ensure steady cybersecurity.

Enlightenment. The purpose of enlightenment programs designed to inculcate new models of application and work to users is determined. The owner of the information, the user of the information and the persons managing the information system are responsible for electronic security. Since the above-mentioned cover a wide range of people, it would be correct to say that everyone is responsible for ensuring electronic security.

Cooperation. The private and government sectors should work in close cooperation to implement cybersecurity strategies. Cooperation should be realized through the exchange of information and advanced experience, as well as the state level trainings. Relevant mechanisms should also be identified to enable interested parties, such as the public and government sectors, to discuss and approve policies on cybersecurity problems. International cooperation is vital because everyone depends on cyberspace, and cybersecurity gaps in one country can affect other countries. But in cooperation with foreign countries in this strategic area, there are also risks for economic, political and national security. International cooperation can cover such areas as legislative activities, incident response, scientific research, hardware and software certification.

It provides for the development of state capabilities and the definition of the necessary legal framework for joining the international fight against cybercrime. In some strategies, cybercrime is paid special attention (Luiijf et. Al., 2011).

After massive cyberattacks on Estonia's network system in 2007, the NATO summit in Bucharest in 2008 determined to take measures against cyberattacks and establish security centers for cooperation in the field of cybersecurity. At this meeting, it was stated that ensuring cybersecurity is first and foremost the responsibility of States. However, after the proliferation of weapons of mass destruction and terrorism, threats from cyberspace were classified as threats aimed at NATO countries at the NATO Summit in Lisbon in 2010. NATO has already developed such documents as "Policy on Cyber Defense" and " Concept on Cyber Defense". But these documents are confidential, only summary information is available on the organization's official website. When defining cybersecurity principles, alliance members relied on the principles of allied solidarity and national sovereignty recognition. The main goal is for all NATO allies to be prepared for cyberattacks and to support one another during such attacks. In order to o attain this goal, allies must improve cybersecurity capabilities in their countries. In this context, networks of close bilateral and multilateral cooperation are being created between partner countries under the auspices of NATO (Klimburg, 2012, p. 253).

It would be nice to emphasize that recent events in Estonia and Georgia have practically proved that the e-government project is in dire need of serious defense capabilities.

It is vital to think clearly about the strict organization of the e-government protection system, since the geospatial factor in which we are located must be taken into

account. During the Russian-Georgian war in 2008, hacker groups of Russian special services hacked all Georgian news sites, as well as all portals with the domain ".ge". Only the domain of the Ministry of Foreign Affairs of Georgia, which is hosted on Estonian servers, was not affected by this attack. Estonia has also previously faced a devastating Russian attack in this regard, so Azerbaijan can already benefit from Estonia, which has huge experience in the field of cybersecurity.

Each state has a different approach to cybersecurity, there are such views on cybersecurity as information security, the issue of national security, the issue of law enforcement agencies and the economic issue. Although all countries recognize the importance of international cooperation in the field of cybersecurity, the lack of a common language and approach complicates the process of international cooperation. Therefore, the partnership and cooperation of countries in the field of cybersecurity is vital.

Provision of reliable cybersecurity is beyond the access of small states independently, and solving this problem requires the partnership and cooperation of all interested parties - states, law enforcement agencies, the private sector and citizens. The cross-border nature of cyber threats encourages countries to work closely together in the field of cybersecurity.

Results

Nowadays, the issue of cybersecurity is becoming a national strategic problem and affects all sectors of society. Fast, efficient and effective fight against cyber threats requires the definition of the right strategic goals. The development of a national cybersecurity strategy is the first and main step in the fight against cyber threats. To develop a successful and optimal national cybersecurity strategy, available national cybersecurity strategies should be analyzed and successful practices against cyber threats should be used.

BIBLIOGRAPHY

[1] Hasanov, A.H. (2106). Factors determining the importance of creating a cyber army in the Armed Forces of the Republic of Azerbaijan. National Security and Military Sciences, No. 2.

[2] Hasanov A.H., Iskandarov X.I. (2017). NATO's Cybersecurity Policy and Azerbaijan. National Security and Military Sciences, Baku, No 2 (3).

[3] Imamverdiyev Y.N. (2013). Analysis of national cybersecurity strategies, "I Republican scientific--practical conference on information security problems" dedicated to the 90th anniversary of the national leader of the Azerbaijani people Heydar Aliyev, May 17-18, p. 14-17.

[4] Sood A.K., Enbody R.J. (2013). Targeted cyberattacks: a superset of advanced persistent threats / IEEE Security & Privacy, 2013, Vol. 11, No. 1.

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

[6] US Government Accountability Office. (2009) National cybersecurity strategy: Key Improvements are Needed to Strengthen the Nation's Posture, GAO-09-432T.

[7] Mitra A., Schwartz R.L., From cyber space to cybernetic space: rethinking the relationship between real and virtual spaces // Journal of Computer-Mediated Communication's, 2001, Vol. 7, No. 1. http://jcmc.indiana.edu/vol7/issue1/mitra.html [access: 11.02.2022].

[8] National Audit Office. (2013). The UK cyber security strategy: Landscape review, February.

[9] ENISA. (2012). National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace.

[10] Chałubińska-Jentkiewicz K., Radoniewicz F., Zieliński T. (2022). Cybersecurity in Poland Legal Aspects.

[11] Ministry of Digital Affairs (2019). Cybersecurıty Strategy of The Republıc of Poland for 2019-2024, https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8 [access: 11.02.2022].

[12] Resmi Gazete (2013). National Cyber Security Strategy and Action Plan for 2013-2014. www.resmigazete.gov.tr [access: 11.02.2022].

[13] Klimburg, A. (Ed.) (2012). National cyber security framework manual, NATO CCD COE Publication,Tallinn.