Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 116-122

UOT 351/354 DOI: 10.30546/9878.2024.2.10.0034.

THE IMPORTANCE OF CYBER DEFENSE FOR AZERBAIJANI NATIONAL SECURITY

mayor Mehrac Huseynov
National Defence University
mehrac77@yahoo.com

Abstract. This article offers a comprehensive exploration of cyber defense's significance for Azerbaijan's national security across three sections. The first section outlines Azerbaijan's importance and recent developments in cyberspace. The second section delves into the Baku-Tbilisi-Ceyhan Pipeline Cyber Attack case study, analyzing its execution, focus on national power elements, and consequential impacts through diplomatic, informational, military, and economic lenses. Finally, the third section provides insights into necessary capabilities to enhance Azerbaijan's cyber defense posture.

The purpose of this research is to assess the importance of cybersecurity in bolstering Azerbaijan's national security framework, with a specific focus on recent developments and vulnerabilities in cyberspace. A combination of analysis and synthesis research methods is employed, including literature review, case study analysis, stakeholder interviews, comparative analysis, and scenario planning. These methods enable a comprehensive examination of cybersecurity in Azerbaijan, encompassing existing literature, in-depth case studies such as the Baku-Tbilisi-Ceyhan Pipeline Cyber Attack, stakeholder insights, comparative assessments with other nations, and scenario-based analysis to anticipate cyber threats. The research yields crucial findings, emphasizing the necessity for robust cybersecurity measures in Azerbaijan due to its escalating reliance on cyberspace and the vulnerabilities exposed by incidents like the Baku-Tbilisi-Ceyhan Pipeline Cyber Attack. Furthermore, it underscores the interconnected nature of cyber threats across diplomatic, informational, military, and economic domains, advocating for investments in technology, human capital, and international collaboration to fortify Azerbaijan's cyber defence posture and enhance cyber resilience.

Keywords: cybersecurity, Baku-Tbilisi-Ceyhan Pipeline, geopolitics, cyber threats, national security

Introduction

The Republic of Azerbaijan is located at the crossroads of Eastern Europe and Western Asia. “Despite its limited size and small population, Azerbaijan, with its vast energy resources, is also geopolitically critical. It is the cork in the bottle containing the riches of the Caspian Sea basin and Central Asia” [1].

Despite the political chaos and economic paralysis created by the collapse of the Soviet Union in the early 1990s and the recently ended conflict in the Karabakh region, Azerbaijan's economy has experienced a significant transformation and development. The economy of Azerbaijan is based on oil and natural gas, and the Baku-Tbilisi-Ceyhan Oil Pipeline is one of the biggest post-Soviet government projects. It is one of the leading projects that increased Azerbaijan’s geopolitical importance, was constructed to carry Azerbaijani oil to the west, and was completed in 2005. As a result, Azerbaijan is the most powerful country in the Caucasus region economically and militarily. However, economic improvement and strengthening of the infrastructure has created many challenges and threats. The country's location and its natural resources, coupled with its balanced policy to be neutral and cooperate with both the East and West, makes Azerbaijan vulnerable as a geopolitical pivot. Azerbaijan tries to maintain its status as a sovereign and independent country by avoiding alliances with any geopolitical bloc, but instead opts for economic, energy, and military cooperation with both West and East [2]. This economic development brought information technology to the country and made its infrastructure basically digital. The digitization of the functions and structures of state institutions and private

companies provides many benefits to the government, businesses, customers, and citizens. However, the ever-increasing use of information and communication technology moved society into the rapidly evolving cyber world. This transformation shows all the institutions, organizations, and functions of the society, and how the systems and processes of society are constructed and executed. The information and technology connected to the cyber environment are vulnerable to various security threats. Hence, the security of information as well as the security of the technology structures and infrastructure systems has become a serious issue. The State Security Service of Azerbaijan believes that the cyber-security threats are prevailing in Azerbaijan due to the digitalization of society and the development of non-oil state infrastructure [3].

Baku-Tbilisi-Ceyhan (BTC) Pipeline Cyber Attack

The term cyberspace is not only associated with the internet and connected computer systems, but it is also linked with the electronic devices and the systems connected directly or indirectly to it [4]. The security of cyberspace usually refers to the protection of cyberspace infrastructure, which contains the four features, computer hardware, telecommunication structure, the control systems of operating devices, and digital devices such as laptops or desktop computers [4]. Science fiction society termed the word, cyberspace, and now it is a mainstream term used to describe the domain of the global information technology environment.

We live in an increasingly networked world, from personal banking to government infrastructure. Protecting these networks is no longer optional; instead, it is mandatory and requires a great deal of investment. [5] Moreover, it is not only about the investment in technology, but also about personal awareness and about how to remain secure in cyberspace. Cyber security has become a primary challenge to all countries and organizations. It consists of threats that are generally unknown to the public and is strongly connected to strategic interests and information security.

Due to increased dependence on the availability of information communication technologies and the ever-growing number of internet users (now 40 percent of the world’s population) cyber security is now much more important in the world. Statistics and reports show that cyber threats are on the rise. The potential yearly financial impact on the global economy due to cybercrime exceeds $455 billion. [6] Developing countries are most at risk to cyber-attacks due to the broader use of information and communication technologies. Security is crucial for the socio-economic wellbeing of a country in the adoption of new technologies. Considering that Azerbaijan is among developing countries and uses the latest technologies in the field of energy, it is inevitable that cyber security is important for the country.

Traditional security has always been a priority of Azerbaijan’s foreign and domestic policies due to the Armenian occupation of Nagorno-Karabakh, which has recently ended, concerns about the Caspian Sea’s energy security, and the antagonistic neighbouring states of clerical Iran and nuclear Russia. However, the well-known Stuxnet case, which aimed to delay the Iranian nuclear program, focused Azerbaijan’s and other affected world states’ attention on cyber security [3]. Stuxnet mainly targeted Iranian computers; however, it also affected other states. Even though this incident did not severely damage the infrastructure and the economy, it showed the existing cyber security gaps in Azerbaijan. In Azerbaijan, the legal basis for cyber security should be strengthened because cyber weapons (such as the Stuxnet virus) have attempted to destroy the government infrastructures. Economic development and neighbouring threats on the borders show the significance of cyber security in all critical areas. Hence, cyber security has become vital concern to protect Azerbaijan's national security.

Baku-Tbilisi-Ceyhan (BTC) pipeline carries oil from Caspian Sea across Azerbaijan, Georgia and Turkey. The Sangachal terminal situated on the Caspian Sea coastline within Azerbaijan's borders is connected to the Ceyhan marine terminal located along the Turkish Mediterranean coast. Moreover, the pipeline facilitates the transportation of crude oil from Turkmenistan. Since October 2013, it has also recommenced the conveyance of Tengiz crude oil from Kazakhstan via the BTC pipeline [7]. The pipeline, which commenced operations in June 2006, was constructed by the Baku-Tbilisi-Ceyhan pipeline company, which is operated by British Petroleum.

The BTC pipeline incident is associated with the cyber-attack that took place on August 6, 2008, in close proximity to the town of Refahiye within Turkey. Hackers planned a combined physical and cyber-attack on the pipeline that caused an explosion and fire with flames as high as 50 meters [8]. The cyberattack carried out in 2008 on the BTC oil pipeline on Turkish soil created an explosion that ignited a fire, which blazed for over 20 days. Along the way, millions of dollars were lost in material and revenue. The physical rupture, which led to an explosion that resulted in a fire that was extinguished by firefighters on 7 August 2008. The pipeline was out of commission until reopened on 25 August 2008 [8].

The Kurdistan Workers' Party (PKK) terrorist group, battling with Turkey since 1984, claimed responsibility for the attack [9]. Despite the fact that PKK claimed responsibility for the attack, another interesting fact was that the incidence happened during a period of escalating tensions between Russia and Georgia, leading toward the brink of armed conflict. Two days after the pipeline explosion, Russia formally deployed troops into the Russian-Georgian conflict. The BTC pipeline runs through Georgia and it represented a threat to Russia's energy policy. In some reports, it was observed that attackers consisted of a team of two with laptops near the pipeline [8].

The BTC pipeline has been reported to have a new IP-based camera system network along the pipeline. The attack was made through an unprotected wireless network, making disconnections of security alarms and survey cameras. Cyber attackers had access to the control system of the pipeline and suppressed the alarms, manipulated the process and blunted the system operators [8]. Although the control systems in use at the BTC pipeline have not been disclosed, it is reasonable to assume that the security of the pipeline was very weak and the only observation of the pipeline occurred through the surveillance camera network installed along the pipeline and linked to the surveillance centre via the internet. The attackers identified these weaknesses and were able to exploit these vulnerabilities and penetrate the technical control system to access the alarm management server [9]. After disabling the alarms and all communication tools with local teams (by interfering with wireless communication,) they took control of industrial systems and created excessive pressure resulting in an explosion in the pipeline [9]. The described attack scenario is lacking details, but reports suggests that the attackers might have used a wireless Internet connection to gain access to the security camera network. Other details indicate physical access to field controllers may have also been necessary [8].

The scenario describes the attack as targeting industrial computers at valve stations to change pressure and misreport results back to the control room [8]. This information may point to direct physical access to control components at remote locations. This information suggests that there was direct physical access to control components at remote locations. The assault on the camera system might have solely aimed to obstruct the pipeline operator's view, potentially facilitating physical intrusions to gain access to field components.

This event is an example of an industrial system attack, which may have been partly supported by a foreign government. When we analyse this attack from the Diplomatic, Information, Military, and Economic (DIME) perspective, the most affected national power was economy. Three elements of national power were covered in one paragraph.

Diplomatic-Information-Military: PKK's proclamation and the rise of Russian – Georgian tensions infer that Diplomatic issues may have been the basis of this attack but tangible evidence that can prove it does not exist. In addition, no observable diplomatic consequence arose from this attack other than the proclamation of PKK's responsibility for the attack. Generally, it is known that PKK's aim is getting diplomatic power in Turkey and divide the country as they represent themselves as freedom fighters of the Kurdish population. It is possible that they tried to send a message to the Turkish government with this attack by demonstrating their capabilities. Countries and companies are strong as long as they are able to hide their information and secrets, which they have to protect. Damaging these institutions and countries is going to be a great deal easier when they are unable to defend critical information and infrastructure. A terrorist organization attacking an industrial system with a combination

of physical and cyber-attacks, demonstrates advanced capabilities perhaps associated with a military, but none of these attacks were aimed at a specific military installation.

Economic: The researcher would like to start the analysis with BCT throughput capacity – one million barrels per day from March 2006 to March 2009 [7]. The pipeline has significantly boosted the economies of the host countries, as Georgia and Turkey receive substantial annual transit fees, amounting to large sums of money. In the early years of operation, Turkey is anticipated to receive around $200 million annually in transit fees, with projections suggesting that these fees could rise to $290 million per year from 2017 to 2040. Additionally, Turkey gains from heightened commercial activity in the port of Ceyhan and other areas of eastern Anatolia, a region that had witnessed a notable decline in economic activities since the Gulf War in 1991 [10]. This data shows us how big the economic damage is in this attack. If one only takes into consideration the transfer fee lost, it is approximately equal to $11 million USD.

On the other hand, Georgia and Azerbaijan also were affected economically by this attack. Georgia is projected to receive an average of $62.5 million annually in transit fees [10]. Twenty-day downtime means about $3.5 million loss of income for Georgia. This attack also created a significant economic loss for Azerbaijan. As mentioned earlier, one million barrels per day of oil were flowing through BTC; this means that the 20-day interruption caused 20 million barrels of oil loss.

What capabilities are needed to improve Azerbaijan's cyber defence posture?

The purpose of this paragraph is to answer: What capabilities are needed to improve Azerbaijan's cyber defence posture? This question has been answered under four main headings: Improve Education on Cyber-Security, Awareness of Cyber Situations, Cyber-Security Partnerships, and Strong Cyber-Deterrence.

To improve education on cyber-security, basic cyber security should be taught at the school level, from beginning levels to university level. Training programs should focus on increasing the number of incident response teams. Education would focus on prevention of attacks and key is a strong defence. Prevention is expensive in terms of time and money but recovery is very costly and international credibility cannot be rebuilt overnight. Cyber hygiene courses should be created for the governmental entities and should be mandatory for all employees as a prerequisite course.

If Azerbaijan does not know who the attacker is (successfully or unsuccessfully), Azerbaijan cannot protect itself. New laws should require that certain types of cyber-incidents must be reported to appropriate authorities. Government policy must incentivize and encourage sharing of attack data by victims, not inhibit or unnecessarily penalize/publicize. A framework must be built to predict the impact of new cyber-attacks on other parts of the Azerbaijan internet infrastructure in order to take immediate corrective action.

Cyber-Security Partnerships must be made. Cyber-defence partners could include Turkey, Georgia as well as Pakistan. Due to sharing BTC pipeline and other strategic planned projects, with Turkey and Georgia, it is inevitable to create partnerships in cyberspace. On the other hand, Pakistan is one of the most powerful military partners of Azerbaijan and relations at government level are based on very strong ties.

Strong cyber-deterrence is important and robust cyber-attack capability must be created. Respondents must know that Azerbaijan has strong cyber-deterrence capabilities. Cyber threats can be categorized in many ways, and each category will have different motivations and cyber skills or abilities. The government's ability to deter each cyber-hostile group should be variable.

Over all DIME Analysis showed that, cyber threat is very harmful and very possible for Azerbaijan due to its industrial-based economy. In order to protect the industrial-based economy and infrastructure against cyber-attacks, cyber defence has vital importance in the national security of Azerbaijan. Moreover, analysis has shown that the most affected instrument of national power in possible cyber-attacks to Azerbaijan is the economy. National defence measures will mitigate the damage of cyber hazards. First of all, it can be ensured that the critical infrastructures of country work with the network

independent of the internet. The intranet system can be implemented to prevent attacks from the internet. National security policy should be determined and local software should be created and focused on that. The software produced by the foreign country may not be secure. In critical infrastructure systems and software, the possibility of espionage can be weakened by using national products. In order to identify vulnerabilities and hazards, attack threat detection mechanisms should be used and strengthened. General participation can be achieved by emphasizing the importance of national cyber exercises. The support of universities and private institutions in cyber defence strategies must be increased. National Strategy, Laws and Recommendations, and cooperation with partner countries are important factors in increasing the country's cyber power.

In conclusion, the Republic of Azerbaijan stands at a critical juncture, balancing its geopolitical significance as an energy hub with the increasing challenges posed by cyber threats. The country's economic transformation, driven by its oil and natural gas resources, has elevated its status in the Caucasus region. However, this development has exposed Azerbaijan to vulnerabilities in the rapidly evolving cyber world.

The Baku-Tbilisi-Ceyhan (BTC) pipeline cyber-attack serves as a poignant example of the potential risks Azerbaijan faces in the digital era. The combined physical and cyber assault orchestrated by the PKK terrorist group not only caused a significant economic setback but also underscored the weaknesses in Azerbaijan's cyber security infrastructure. This incident emphasizes the need for a robust cyber defense posture to safeguard the nation's critical assets.

Conclusion

Azerbaijan's response to cyber threats requires a multifaceted approach. Primarily, enhancing education on cyber security from schools to universities is imperative. Building a skilled workforce and incident response teams will contribute to preventing and mitigating cyber-attacks. Additionally, fostering awareness of cyber situations and implementing reporting mechanisms for cyber incidents are crucial steps in bolstering the nation's cyber resilience.

Cyber-security partnerships with neighboring countries like Turkey, Georgia, and strong allies such as Pakistan are essential. Given the interconnectedness in the region, collaborative efforts can strengthen collective defenses and provide a united front against cyber threats. Moreover, establishing a strong cyber-deterrence capability is paramount. Azerbaijan must highlight its ability to defend against cyber-attacks, thereby dissuading potential adversaries.

The Diplomatic, Information, Military, and Economic (DIME) analysis underscores the economic repercussions of cyber-attacks on Azerbaijan. The country's industrial-based economy makes it susceptible to disruptions, and protecting against cyber threats becomes integral to national security.

In conclusion, Azerbaijan's journey towards economic development and geopolitical prominence necessitates a proactive and comprehensive approach to cyber security. By investing in education, fostering awareness, building strategic partnerships, and establishing a formidable cyber-deterrence capability, Azerbaijan can fortify its defenses in the cyber domain. In doing so, the nation can continue to thrive in the digital age while safeguarding its critical infrastructure and economic prosperity.

References

1. Brezinski, Z. The Grand Chessboard. American Primacy and Its Geostrategic Imperatives / Z.Brezinski – NY: Basic Books – 1997. – 240 p.

2. Strîmbovschi, S. Azerbaijan’s Balanced Foreign Policy Trapped in a Volatile Geopolitical Context: [Electronic resource] / – europolity.eu. – Bucharest, Romania, 2015.
URL: http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.121-134.pdf

3. Makili-Aliyev, K and Attiq-ur-Rehman. Cyber-security objective: Azerbaijan in the digitalized world: [Electronic resource] / – sam.az. – November 2013.

URL:http://sam.az/uploads/PDF/SAM%20comments%20and%20review%20publications/Cyber%20Security%20objective%20Azerbaijan%20in%20the%20digitalized%20world.pdf.

4. Fischer, E.A. Creating a National Framework for Cybersecurity: An analysis of issues and options / E.A. Fischer. – New York: Nova Science Publishers, – 2019. – 92 p.

5. Detlev, G., Bertrand, L., Orzechowski, D. Cyber risk: Why cyber security is important: [Electronic resource] / – coursehero.com, – 2019.
URL:https://www.coursehero.com/file/42218407/Explain-What-Cybersecurity-Is-and-Why-We-Should-Care-revisiondocx/

6. Reuters. Cyber security: [Electronic resource] / – reuters.com. – 10 December, 2018.
URL:https://www.reuters.com/article/us-cybersecurity-mcafee-csis/cyber-crime-costs-global-economy-445-billion-a-year-report-idUSKBN0EK0SV20140609

7. BP.com. Baku-Tbilisi-Ceyhan pipeline: [Electronic resource] / – bp.com.
URL: https://www.bp.com/en_az/caspian/operationsprojects/pipelines/BTC.html.

8. Lee, R.M, Assante. M.J., Conway T. Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack: [Electronic resource] / – ICS Defense Use Case (DUC.) SANS Institute. – Bethesda, MD, USA, 20 December, 2014.
URL:https://scholar.google.com/citations?view_op=view_citation&hl=en&user=mqu2hhyaaaaj&citation_for_view=mqu2hhyaaaaj:mvmsd5a6bfqc

9. The Sentryo Files: Industries vs. cyber-attacks Episode 2. Attack on the BTC oil pipeline in 2008: [Electronic resource] / – Sentryo.net. – 17 August, 2017.
URL: https://www.sentryo.net/the-sentryo-files-industries-vs-cyberattacksepisode-2-attack-on-the-btc-oil-pipeline-in-2008/.

10. Iqbal, M. Z., Shah, N. The Baku-Tbilisi-Ceyhan Pipeline: Political and Economic Impacts for the Region // – Islamabad: Pakistan Horizon, – 2015. № 68(1). – p. 69-81.

Xülasə
Azərbaycanın milli təhlükəsizliyi üçün kibermüdafiənin əhəmiyyəti
Mehrac Hüseynov

Məqalənin hər üç bölməsində Azərbaycanın milli təhlükəsizliyi üçün kibermüdafiənin əhəmiyyətinin hərtərəfli tədqiqi əks olunur. Birinci bölmədə son illərdə kiberməkanda baş verən hadisələr vurğulanır. İkinci bölmədə Bakı–Tbilisi–Ceyhan boru kəmərinə kiberhücum araşdırılır, diplomatik, informasiya, hərbi və iqtisadi milli güc elementləri də nəzərə alınaraq, bu hücumun təsiri təhlil edilir. Üçüncü bölmədə Azərbaycanın kibermüdafiə sahəsindəki gücünün artırılması üçün lazım olan imkanlar barədə məlumatlar öz əksini tapır. Tədqiqat işində məqsəd Azərbaycanın milli təhlükəsizlik sisteminin gücləndirilməsində kibertəhlükəsizliyin əhəmiyyətini vurğulamaq, kiberməkanda baş verən son hadisələri qiymətləndirmək və bu sahədəki zəiflikləri müəyyən etməkdən ibarətdir. Məqalədə təhlil, sintez və müqayisəli təhlil tədqiqat metodlarından istifadə edilmişdir. Bu üsullar Azərbaycanda kibertəhlükəsizliyin hərtərəfli tədqiqinə, mövcud ədəbiyyatların təhlilinə, Bakı–Tbilisi–Ceyhan boru kəmərinə edilən kiberhücumun analizinə, maraqlı tərəflərin rəylərinə, digər ölkələrlə müqayisəli qiymətləndirmə aparmağa və ssenari əsasında təhlilə imkan verir. Tədqiqat işində kiberzəifliklərin ağır nəticələrinin qarşısının alınmasında kibertəhlükəsizlik tədbirlərinə ehtiyac olduğu vurğulanır və bununla bağlı tədbirlər planı təklif edilir. Bundan əlavə, tədqiqat işində diplomatik, informasiya, hərbi və iqtisadi sahələrdə kibertəhlükələrin bir-biri ilə əlaqəli xarakteri, eyni zamanda Azərbaycanın kibermüdafiə imkanlarını gücləndirmək və kiberdavamlılığını artırmaq üçün texnologiyaya, insan kapitalına və beynəlxalq əməkdaşlığa sərmayələrin yatırılmasının əhəmiyyəti əsaslandırılır.

Açar sözlər: kibertəhlükəsizlik, Bakı-Tbilisi-Ceyhan boru kəməri, geosiyasət, kibertəhdidlər, milli təhlükəsizlik

Аннотация
Значение киберзащиты для национальной безопасности Азербайджана
Мехрадж Гусейнов

В данной статье в трех разделах описывается комплексное исследование значимости киберзащиты для национальной безопасности Азербайджана. В первом разделе отражается важность Азербайджана и развития в киберпространстве за последние годы. Во втором разделе рассматривается пример кибератаки на трубопровод Баку-Тбилиси-Джейхан, анализируется ее реализация, основное внимание уделяется элементам национальной мощи и полученным эффектам через дипломатическую, информационную, военную и экономическую призму. И наконец, в третьем разделе дается представление о необходимых возможностях для укрепления потенциала киберзащиты Азербайджана. Целью данного исследования является оценка значимости кибербезопасности в укреплении системы национальной безопасности Азербайджана, с особым акцентом на последние события и уязвимости в киберпространстве. В анализе и синтезе используется сочетание исследовательских методов, включая анализ литературы и работы, интервью с заинтересованными сторонами, сравнительный анализ и сценарное планирование. Эти методы позволяют провести всестороннее исследование кибербезопасности в Азербайджане, проанализировать существующую литературу, углубленные тематические исследования, такие как кибератака на трубопровод Баку-Тбилиси-Джейхан, мнения заинтересованных сторон, сравнительные оценки с другими странами, а также анализ на основе сценариев для преждевременного прогнозирования кибербезопасности. Исследование дает важные результаты, которые подчеркивают необходимость принятия строгих мер по кибербезопасности из-за уязвимостей, трубопровода Баку-Тбилиси-Джейхан подверженных инцидентам кибератак в Азербайджане и уязвимости к кибератакам. Кроме того, он подчеркивает взаимосвязанный характер киберугроз в дипломатической, информационной, военной и экономической сферах, пропагандируя инвестиции в технологии, человеческий капитал и международное сотрудничество для укрепления потенциала киберзащиты Азербайджана и повышения киберустойчивости.

Ключевые слова: кибербезопасность, трубопровод Баку-Тбилиси-Джейхан, геополитика, киберугрозы, национальная безопасность

Məqalə redaksiyaya daxil olmuşdur: 15.01.2024
Təkrar işlənməyə göndərilmişdir: 26.01.2024
Çapa qəbul edilmişdir: 07.03.2024