МРНТИ 20.15.05. https://doi.org/10.58805/kazutb.v.1.22-320

CYBER TECHNOLOGIES IN MODERN INTERNATIONAL CONFLICTS AND METHODS OF ENSURING CYBERSECURITY

R.I.Vekilov[1*], B.T.Baiserkeeva[2],
[1]Armed Forces of the Republic of Azerbaijan, Baku, Azerbaijan,
[2]Academy of Civil Aviation, Almaty, Kazakhstan,
e-mail: rasimvekilov757@gmail.com

The article examines the problems of cybersecurity of the state. As you know, the number and scale of international conflicts have increased recently. The methods of conducting armed conflicts have also changed. More and more people began to move from conventional military clashes to information wars and cyber wars. Over time, technological progress has led to the emergence of new arenas for conflicts between countries and factions. Cyberwar has become one of these arenas, where the main weapons are not missiles and submachine guns, but computer codes and supercomputers. This article reveals the role of cyber technologies in modern international conflicts and presents what threats and opportunities they provide on the battlefield.

Keywords: cyberattacks, cybersecurity, cyberwarfare, codes, threats, digital technologies, information flows, disinformation.

КИБЕРТЕХНОЛОГИИ В СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ КОНФЛИКТАХ И МЕТОДЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Р.И Векилов[1*], Б.Т.Байсеркеева[2],
ВС Республики Азербайджан, г. Баку, Азербайджан,
Академии гражданской авиации, г. Алматы, Казахстан,
e-mail: rasimvekilov757@gmail.com

В статье исследуются проблемы кибербезопасности государства. Как известно в последнее время увеличилось количество и масштабы международных конфликтов. Также изменились и методы ведения вооруженных конфликтов. От обычных военных столкновений все больше стали переходить к информационным войнам и кибервойнам. С течением времени, технологический прогресс привел к появлению новых арен для конфликтов между странами и группировками. Одной из таких арен стала кибервойна, где основными орудиями стали не ракеты и автоматы, а компьютерные коды и суперкомпьютеры. В этой статье раскрываются роль кибертехнологий в современных международных конфликтах и представлены какие угрозы и возможности они предоставляют на поле войны.

Ключевые слова: кибератаки, кибербезопасность, кибервойны, коды, угрозы, цифровые технологии, информационные потоки, дезинформация.

ҚАЗІРГІ ХАЛЫҚАРАЛЫҚ ҚАҚТЫҒЫСТАРДАҒЫ КИБЕРТЕХНОЛОГИЯ ЖӘНЕ КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ

Р.И.Векилов[1*], Байсеркеева Б.Т[2],
Әзірбайжан Республикасы Қарулы Күштері, Баку, Әзірбайжан,
Азаматтық авиация академиясы, Алматы, Қазақстан,
e-mail: rasimvekilov757@gmail.com

Мақалада мемлекеттің киберқауіпсіздік мәселелері қарастырылады. Өздеріңіз білетіндей, соңғы кездерінде халықаралық қақтығыстардың саны мен ауқымы артты. Қарулы қақтығыстарды жүргізу әдістері де өзгерді. Кәдімгі әскери қақтығыстардан бастап ақпараттық соғыстар мен кибер соғыстарға көшу басталды. Уақыт өте келе, технологиялық прогресс елдер мен топтар арасындағы қақтығыстардың жаңа ареналарына әкелді. Осындай ареналардың бірі кибер соғыс болды, онда негізгі зеңбіректер зымырандар мен автоматтар емес, компьютерлік кодтар мен суперкомпьютерлер болды. Бұл мақалада қазіргі заманғы халықаралық қақтығыстардағы кибертехнологияның рөлі ашылады және олар соғыс алаңында қандай қауіптер мен мүмкіндіктерді ұсынады.

Түйін сөздер: кибершабуылдар, киберқауіпсіздік, кибершабуылдар, кодтар, қауіптер, цифрлық технологиялар, ақпараттық ағындар, жалған ақпарат.

Introduction. Information and cyber wars have become iconic phenomena of the 21st century, when conflicts between states and organizations are increasingly moving into the digital sphere. To understand their significance for the world community and possible consequences, it is necessary to delve more deeply and methodically into the essence of these concepts, to study their basic principles on which they are based. Information warfare refers to conflicts where the key tools are the control of information flows, the spread of disinformation and propaganda. It is carried out with different goals, both geopolitical and ideological, as well as economic. The main influence of information wars is on the mass consciousness, their task is to form public opinion and incline sympathies towards one or another participant in the conflict.

Materials and methods. Cyber wars use computer technology and networks to conduct military operations. Targeted cyber attacks can target critical infrastructure, communications networks, control systems, defense structures and other key enemy facilities. Cyber warfare operations can include espionage, hacking, destabilization of computer systems, and distribution of unwanted software. Cyber wars are often also aimed at creating chaos and panic among the enemy's population or disrupting the vital activity of the country [1].

Consequences of information and cyber wars:

1. Destabilization of countries and regions: information and cyber wars can lead to serious economic and political crises, often accompanied by mass riots.

2. Increasing tension between states: cyber attacks and interference in the affairs of other countries can worsen international relations and provoke unforeseen conflicts.

3. Social and information divide: information and cyber wars can incite hostility and interfaith tension between population groups, slowing down the processes of integration and conflict resolution.

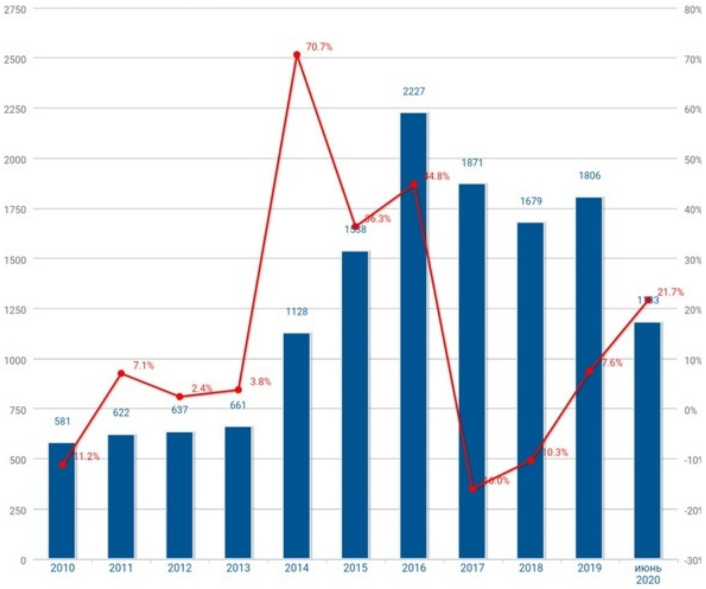

Figure 1 - Cyberattack Growth Chart

Information and cyber wars are important components of modern conflicts, posing a significant threat to peace and stability [2]. They require constant development of defense and counterattack strategies and demonstrate the need for cooperation and coordinated efforts between States in the fight against this new type of hybrid warfare (Fig.1).

Cyber Espionage and hacking of systems

In the context of increasing dependence on digital technologies and Internet connections, cyber espionage and hacking of computer systems have become integral components of modern geopolitical conflicts.

The role of cyber espionage and system hacking in modern conflicts:

1. Intelligence gathering: Cyber espionage allows states and organizations to gain access to classified information of adversaries, such as plans and strategies, data on new technologies or defense resources. This gives a strategic advantage and the opportunity to anticipate and prevent the actions of opponents.

2. Destabilization of infrastructure: hacking of computer systems and infrastructure can leave the enemy without communication, control over key facilities and access to important data. Such attacks can significantly weaken the enemy's defensive capabilities and create suitable conditions for an offensive [3].

3. Psychological warfare: cyberattacks can cause panic and chaos among the enemy's population, weakening their internal stability and morale. In addition, cyber espionage can help identify enemy vulnerabilities for psychological aggression (Fig. 2).

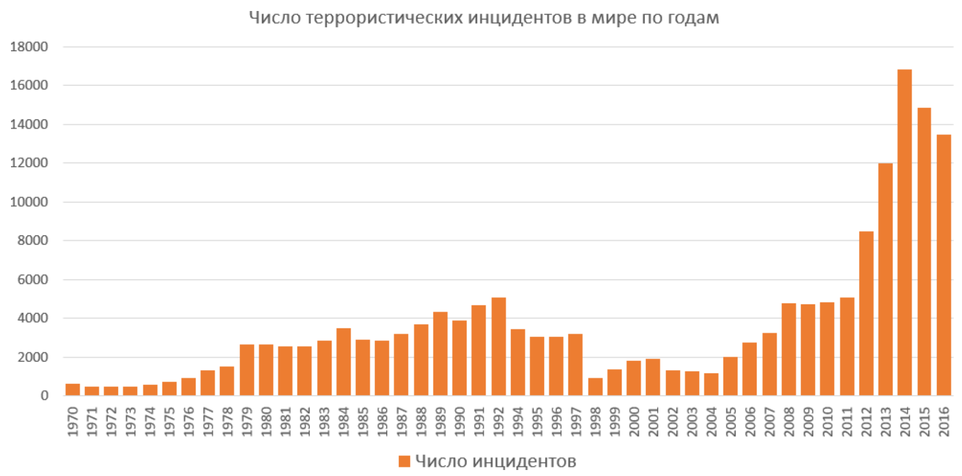

Figure 2 - Diagram of the increase in the number of cyber espionage cases

Discussion of the results. *Methods of cyber espionage and hacking of systems:*

1. Phishing: one of the most common methods of cyber espionage, in which attackers pose as trusted sources and use social engineering approaches to gain access to personal data, passwords and other important information.

2. Malware: Spies use various types of malware that can steal data, track user activity, hack into systems or block access to them.

3. Vulnerability scanning: Attackers constantly analyze and search for vulnerabilities in enemy systems. They use the vulnerabilities found to infiltrate and attack computer and communication networks.

4. Using insiders: spies can recruit people from inside an organization or state to transfer information or give access to systems.

5. Attacks on databases and servers: hackers can gain access to databases and servers, as well as disrupt their operation, steal data or distort information.

Cyber espionage and hacking have become integral elements of modern conflicts and pose a serious security threat. Success in these wars requires States and organizations to pay close attention to the development of cybersecurity strategies and tactics [4]. Only an integrated approach to digital security can give hope for strengthening defense and achieving success in the fight against cyber espionage and hacking of systems (Fig.3).

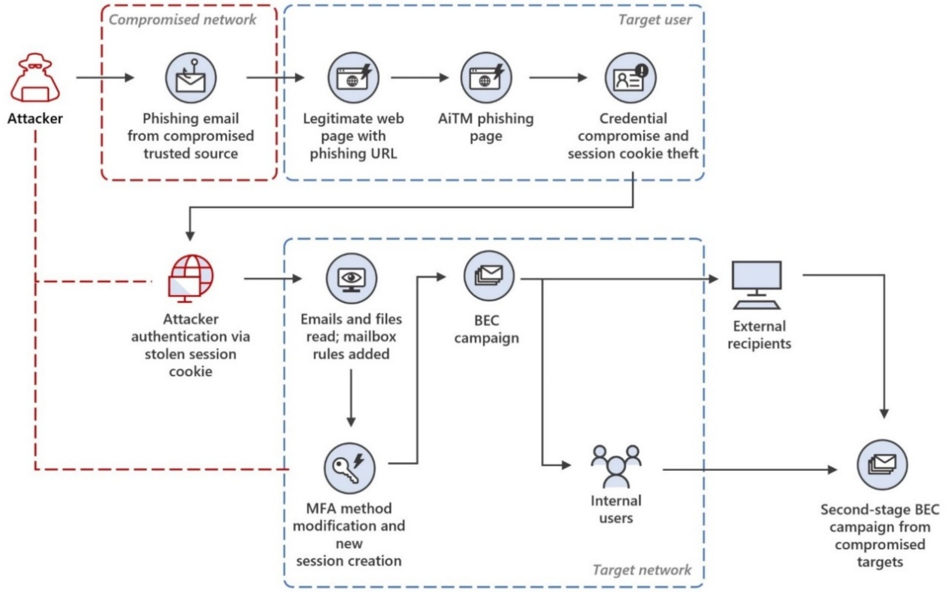
Compromised network
Target user
Attacker
Phishing email from compromised trusted source
Legitimate web page with phishing URL
AiTM phishing page
Credential compromise and session cookie theft
Attacker authentication via stolen session cookie
Emails and files read; mailbox rules added
BEC campaign
External recipients
MFA method modification and new session creation
Internal users
Second-stage BEC campaign from compromised targets
Target network

Figure 3 - Block diagram of the phishing method

In modern cyber conflicts, attacks on critical infrastructure occupy a special place, since such facilities are considered vital for the functioning of States and their economies. Let's consider the goals, methods and consequences of attacks on critical infrastructure in cyberwarfare [5]. Targets of attacks on critical infrastructure:

1. Weakening of the enemy's defensive capabilities: attacks on critical infrastructure can disrupt important defensive systems, resulting in the vulnerability of the enemy to possible threats.

2. Infrastructural and economic chaos: attacks on critical facilities can cause significant problems in the operation of transport systems, electricity, water supply, communications and other services, which will lead to serious economic damage and loss of manageability.

3. Psychological impact: attacks on critical infrastructure create an atmosphere of fear, panic and hopelessness among the population and increase internal political tensions between different groups of society.

Methods of attacks on critical infrastructure:

1. Hacking and access to remote management: Attackers can exploit vulnerabilities in the management and control systems of critical infrastructure to gain access to the management of these objects by hacking.

2. Malicious software: the use of various types of malware to disrupt systems, steal data, introduce deletions and trigger accidents.

3. Denial of Service (DoS) and distributed denial of service (DDoS) attacks: overloading objects and their communication systems or computer networks to ensure their temporary or long-term inoperable state.

4. Physical actions: acts of sabotage, penetration and sabotage in the territory of critical infrastructure, in an attempt to disrupt their functioning.

The consequences of attacks on critical infrastructure

1. Destruction of key facilities: Attacks can result in the destruction or serious damage to the enemy's most important facilities.

2. Economic losses: attacks can result in significant economic damage, as well as temporary or prolonged shutdown of vital systems.

3. The possibility of conflict escalation: provocative actions in cyberspace can provoke an escalation of political and military conflicts, even to the level of armed clashes [6].

*The consequences of attacks on critical infrastructure***.** Attacks on critical infrastructure are one of the key aspects of modern cyber conflicts and require careful study and development of strategies to counter them. To reduce the risk of such attacks, it is necessary to develop cybersecurity systems, raise the level of culture and awareness of cyber threats, as well as improve the domestic and international legislative and legal framework to deter and prevent attacks on critical infrastructure.

Mathematical substantiation of the methodology for monitoring the level of information security. The Pareto Principle is used to compare different techniques. ”Pareto optimality” is as follows: the state of the system in which none of the estimated indicators can be improved without deterioration of another indicator [3]. From the point of view of controlling the level of information security, Pareto optimality can be applied to assess the trade-offs between the costs and benefits of various security measures. For example, more extensive implementation of security measures can increase the level of protection, but also increase the cost of operation.

The optimal solution will be one that provides a given acceptable level of security at a reasonable lowest cost. Pareto optimality can be used to determine the optimal balance between safety and economic efficiency in a given situation. Let's define a set of numerical functions f1, f2... fm, m ≥ 2 defined on the set of possible solutions X as optimality criteria (objective functions). The vector f = (f1, f2, ..., fm) is called a vector criterion that takes values in the m-dimensional space Rm - the space of estimates.

The vector estimate of a possible solution x∈X for the vector criterion f is determined by (1):

$$f(x) = (f1(x), f2(x), \dots fm(x))Rm \qquad (1)$$

All possible vector estimates form a set of possible estimates (2):

$$Y = f(x) = \{y \in Rm \mid y = f(x) \text{ for } x \in X\} \qquad (2)$$

All possible selectable estimates form a set of selectable vectors (estimates) (3):

$$C(Y) = f(C(X)) = \{y \in Y \mid y = f(x) \text{ for } x \in C(X)\} \qquad (3)$$

A multi-criteria task (multi-criteria optimization task - MKO) is called a selection task that includes a set of acceptable values of X and a vector criterion f, or the MKO task consists in finding a set of selectable solutions With(X), such that With(X)⊂X taking into account the preference ratio x based on a given vector criterion f, set in accordance with the goals (preferences) of the decision-maker. It is known that a solution x*∈X is called Pareto optimal (or Pareto-optimal) if there is no such possible solution x∈X for which the inequality f(x) ≥ f(x*) holds.

Cyber operations of military specialists are a set of strategic, tactical and technical measures aimed at using information and digital technologies to ensure national security, conduct intelligence and counterintelligence, protect cyberspace and influence enemy communication systems.

Conclusions. Cyberwar has long ceased to be a fantasy scenario and has become a reality. Today, it plays a key role in modern conflicts and poses new challenges and tasks to the armies of the world. States are striving to adapt to the new threat and are actively developing new tactics, strategies and defense measures to combat cyberwarfare. The future of warfare will certainly be linked to the development of cyber technologies, and only those who are perfectly equipped and armed with new knowledge and skills will be able to guarantee the successful execution of their defensive and offensive operations.

Reference

1.Algoritm vyjavlenija ugroz informacionnoj bezopasnosti v raspredelennyh mul'tiservisnyh setjah organov gosudarstvennogo upravlenija / A. Ju. Puchkov, A. M. Sokolov, S. S. Shirokov, N. N. Prokimnov // Prikladnaja informatika. - 2023. - T. 18, № 2. - S. 85-102. [in Russian].

2.Vasil'ev V. I. Ocenka aktual'nyh ugroz bezopasnosti informacii s pomoshh'ju tehnologii transformerov / V. I. Vasil'ev, A. M. Vul'fin, N. V. Kuchkarova // Voprosy kiberbezopasnosti. - 2022. - № 2. - S. 27-38. [in Russian].

3.Gladkov A. N. Vizualizacija kiberugroz kak aspekt formirovanija kompetencij v oblasti informacionnoj bezopasnosti // Zashhita informacii. Insajd. - 2023. - № 1. - S. 32-37. [in Russian].

4.Ivanov M.V., Sygotina M.Ju., Vahrusheva M.Ju., Nadrshin V.V. Informacionnaja bezopasnost' sovremennogo predprijatija: parol'naja zashhita// Zashhita informacii. Insajd. - 2022. - № 6. - S. 62-66. [in Russian].

5.Nazarov D. M. Osnovy obespechenija bezopasnosti personal'nyh dannyh v organizacii: ucheb. posobie / D. M. Nazarov, K. M. Samatov ; M-vo nauki i vyssh. obrazovanija Ros. Federacii, Ural. gos. jekon. un-t. - Ekaterinburg: Izd-vo Ural. gos. jekon. un-ta, 2019. -118 s. [in Russian].

6.Savin M.V., Kondratenko M.A. Metodika vyjavlenija i ocenki nedopustimyh sobytij na osnove modeli zrelosti upravlenija informacionnoj bezopasnost'ju.//Zashhita informacii. Insajd. - 2023. - № 1. - S. 24-31. [in Russian].

Information about the author

Vakilov R.I.-Senior Assistant to the Military Attaché of the Armed Forces of the Republic of Azerbaijan, Baku, Azerbaijan, e-mail: rasimvekilov757@gmail. e-mail: rasimvekilov757@gmail.com;

Baiserkeeva B.T.-N. Master's student of the Academy of Civil Aviation, Almaty, Kazakhstan, e-mail:

Baiserkeeva1702@mail.ru

Сведения об авторе

Векилов Р.И. - Старший помощник военного атташе вооруженных сил Республики Азербайджан. +77029105873. E-mail: rasimvekilov757@gmail.com;

БайсеркееваБ.Т.-Н.- Магистрант Академии гражданской авиации, Алматы, Казахстан, e-mail:

Baiserkeeva1702@mail.ru