DOI: 10.15849/IJASCA.250330.03

Int. J. Advance Soft Compu. Appl, Vol. 17, No. 1, March 2025
Print ISSN: 2710-1274, Online ISSN: 2074-8523
Copyright © Al-Zaytoonah University of Jordan (ZUJ)

Cybersecurity in Modern Armed Conflicts: Threats and Responses

Oleh Semenenko[1,*], Svitlana Palamarchuk[2], Tetiana Poberezhets[2], Nataliia Palamarchuk[2] and Serhii Mytchenko[3]

[1]Central Research Institute of the Armed Forces of Ukraine, Ukraine
*e-mail: olehsemenenko4@gmail.com
[2]Scientific Center for Communications and Information Technologies, Kruty Heroes Military Institute of Telecommunication and Information Technologies, Ukraine
e-mails: svitlana_palamarchuk@ukr.net; t.poberezhets@meta.ua; natali.palamar@meta.ua
[3]Department of National Security and Defence Strategy, National Defence University of Ukraine, Ukraine
e-mail: researcher_s_mytchenko@ukr.net

Abstract

The purpose of the study is to develop effective information security strategies in the context of modern armed conflicts. Methods of analysis, experiment, and generalisation were used to achieve this goal. Key results include implementing a programme to simulate attacks on classified information, creating a table of analysis of real hacker groups, and a block diagram of cybersecurity in military conflicts. The results of software implementation and visualisation of attacks on military data revealed various threats, the importance of detecting and countering them for the reliability of defence systems. Cyber-attacks on classified data during the war period highlighted the serious impact of cyber threats on important information resources. Information security strategies in armed conflicts are formulated, including threat analysis, preventive measures, increased resistance, incident response, international cooperation, and ongoing assessment. A flexible approach that covers all aspects of cybersecurity determines the success of protection in high-risk situations of armed conflict. Recommendations include improving technological security tools, implementing forecasting and prevention systems, building a cybersecurity culture, systematically updating and adapting to changes in threats and the technology environment. The practical significance of the study is to identify key aspects for developing and improving cybersecurity strategies in the context of military conflicts.

Keywords: *Attacks on military data exchange, digital security, information warfare, military operations, technical security.*

1 Introduction

In today's military landscape, where technology is taking precedence, the study of cybersecurity in the context of armed conflicts is becoming an extremely urgent task. The growing number of cyber-attacks and information aggression in military conflicts indicates that the use of cyberspace is becoming a key aspect of warfare strategies. The study of this topic should identify strategies that will ensure information sustainability and

Received 4 July 2024; Accepted 17 December 2024

responsibility in military conditions, and effectively counter cyber threats in the modern geopolitical context. The research problem arises from a lack of development and incomplete understanding of aspects of the research topic, including the challenges that arise in connection with the evolution of cyber threats and their impact on security in military scenarios. Information system security, cyber espionage, and destructive attacks pose serious threats to national security. Therefore, the study of this issue is extremely important for developing effective cyber defence strategies that consider the specifics of military operations and provide for negative consequences for information security in conflict conditions.

Another research on this topic is worth considering. For example, the purpose of the study [1] was to analyse the role and place of robotic systems in modern wars and armed conflicts, and to define their tasks on the battlefield and develop recommendations to reduce internal and external threats to their development in the Armed Forces of Ukraine (AFU). Research methods included analysis, induction, deduction, synthesis, and peer review. The results identified internal and external threats, and provided recommendations for ensuring the sustainability of their development. Boychenko et al. [2] analysed the public key infrastructure and the national system of electronic trust services of the Armed Forces of Ukraine. The researchers defined the scientific and practical task of developing a technology for providing electronic trust services for processing information with state secrets, clarified the requirements for the public key infrastructure for protecting classified information, and developed the structure of a software and hardware complex for exchanging secret electronic documents in information and communication systems of the Armed Forces of Ukraine.

Bohomia and Kochegarov stressed that cybersecurity is relevant in Ukraine due to its dependence on technologies and information systems, especially in the context of the military conflict in the east of the country [3]. The growing number of cyber-attacks and the use of cloud services make various institutions vulnerable, leading to the need for effective cyber protection [4]. The purpose of the study was to apply cryptographic methods to ensure confidentiality and data protection in cloud services, paying attention to the features of systems and optimal security methods. Ternovyy et al. considered the problems of cyber defence in Ukraine and the role of cyber defence in the Armed Forces [5]. They identified the threat of cyberspace, which can negatively affect the state and its development, and also analysed the lag of Ukraine in the field of information technology and cyber defence in comparison with other countries. The study highlights the importance of cyber defence in both the civil and military spheres.

In turn, Ostrovskyi noted that the tasks of the communications and cybersecurity troops of the Armed Forces of Ukraine are to organise a communication system, interact with other defence forces, and participate in cyber defence [6]. He noted that specialised divisions provide information security, carry out cyber operations and ensure the functioning of the national cybersecurity system. Therefore, on the way to meeting the standards of the North Atlantic Treaty Organisation (NATO), the system of troops must be modernised to effectively perform tasks. The study by Zhyvylo and Dokil focuses on the history of military strategy, which demonstrates the crucial role of innovations such as the inventions of gunpowder and the internal combustion engine, the impact of which covers not only military strategies, but the entire history of the world [7]. The researchers emphasise that the Armed Forces of Ukraine, in particular the communications and cybersecurity troops, play a key role in protecting national security in cyberspace, and conduct capability assessments, considering the methodological approaches of NATO countries and in accordance with the legislation of Ukraine.

Previous studies have already considered various aspects of cybersecurity and military innovation, but questions remain open about the effectiveness of modernising military systems in the context of cyber threats and interaction with other countries. This study aims to address these gaps, in particular, to develop strategies to protect against modern cyber threats and improve military communications and cybersecurity systems to meet international standards and the challenges of modern cyberspace. The purpose of the study is to create effective cybersecurity strategies in the context of current military conflicts.

2 Materials and Methods

Methods of analysis, experiment, and generalisation were chosen to achieve this goal. The analysis was chosen for careful consideration and disclosure of key aspects of armed conflicts and cyber threats. The analysis provided a deeper understanding of the situation, identified the main factors, and determined causal relationships. Using this method, information warfare in the framework of the military conflict between Russia and Ukraine, China and Taiwan, Israel and Iran were investigated. The concepts of information warfare and cyber warfare were also analysed, the impact of stress on cybersecurity professionals, simulation, and agent-based modelling were considered, and changes in information security policy were explored. In addition, certain digital tools and communication technologies were considered, the impact of virtual organisations on the occurrence of conflicts, and the importance of international cooperation was emphasised. The concept of cybersecurity was considered not only from the standpoint of military conflicts, but also in the energy, industrial, space, and marine sectors.

The experimental method was chosen to test the practical effectiveness of the developed cybersecurity strategies. The experiment provided specific data and results that can be objectively evaluated and compared to determine effective approaches. Using this method, a programme for simulating the protection of military information from cyber-attacks was implemented in Java. This application contains the "MilitarySystem" class and the "Main" class, in which the "main" method creates a MilitarySystem object and calls methods to simulate cyber-attacks and increase cyber defence. The "data" variable contains a string about classified information that represents military data. The "attacks" array is an array of types of cyber-attacks, such as distributed denial-of-service (DDoS) attacks, phishing, and malware attacks. The "securityLevel" variable represents the cyber defence level (initially set to 5). The "simulateAttack()" method simulates a cyber-attack. First, it selects a random attack type and power, and then calls the appropriate attack defence method by transmitting the attack power. The "defendDDoS", "defendPhishing", and "defendMalware" methods model protection against various types of attacks. They display messages about protection or loss of information, depending on the strength of the attack and the level of cyber defence. And the "updesecurity(int level)" method increases the level of cyber defence to a certain level. In addition, a table of comparison and analysis of the activity of real hacker groups has been created. In this table, each UAC-group, due to its own competencies, represents a unique entity with characteristic methods, tools, and the number of participants in the team, and is directed to its own human resources potential and has certain target segments.

The use of the generalisation method is substantiated by the need to draw general conclusions and recommendations based on the results obtained. Due to this method, a block diagram of information security strategies in armed conflicts was developed. Generalisation allowed synthesising knowledge and establishing objective principles that can serve as a basis for further cybersecurity strategies. In general, these methods have helped to systematise and analyse various aspects of armed conflicts and cyber threats, providing a deeper understanding of their nature and interaction.

3 Results and Discussion

3.1 General overview of the topic of information security in armed conflicts

Information security in modern military conflicts is a set of measures aimed at protecting information resources, cyber infrastructure, and important military data in the digital space. This broad concept includes the development and application of strategies, technologies, policies, tools, and techniques aimed at preventing, detecting, and recovering from cyber-attacks. In the context of military operations, cybersecurity encompasses measures aimed at ensuring the confidentiality, integrity, and availability of important military information. It also considers measures to protect critical infrastructures, such as communications systems, control systems, energy networks, and other key components that may be targeted by cyber-attacks. Cybersecurity objectives include identifying information threats, developing and implementing security measures, preventing incidents, and effectively responding to cyber violations. In the context of armed conflicts, cybersecurity is becoming an important component of a modern military strategy aimed at protecting national interests and ensuring sustainability in the face of information vulnerability.

Information warfare is an important aspect of modern armed conflicts and is closely linked to cybersecurity [8, 9]. This form of warfare uses information technology and media to achieve strategic goals in military operations. The main goal of information warfare is to influence society, military command and political decisions of the opponent, form public opinion, and create advantages in the information space [10]. Certain advantages and disadvantages of conducting information warfare can be highlighted. Benefits include speed and globality, misinformation, anonymity, and stealth. This type of war allows quickly influencing at the global level through wide access to the media and the Internet. There is an opportunity to influence society and opponents through the spread of disinformation and information manipulation. In addition, it is difficult to establish sources of information influence, which allows carrying out undercover attacks.

The disadvantages of information warfare consist of the following aspects: the possibility of manipulation, cyber threats, and increased tension. Information warfare can lead to massive manipulation of public opinion and influence the adoption of incorrect decisions. And the use of information technologies can lead to cyber-attacks and cybersecurity breaches. In addition, this method of war can deepen tensions between countries and increase the risk of escalation of the conflict. The overall goal of information warfare is to achieve advantages in the military and political space by influencing information flows and public opinion.

3.2 Software implementation and visualisation of attacks on military data

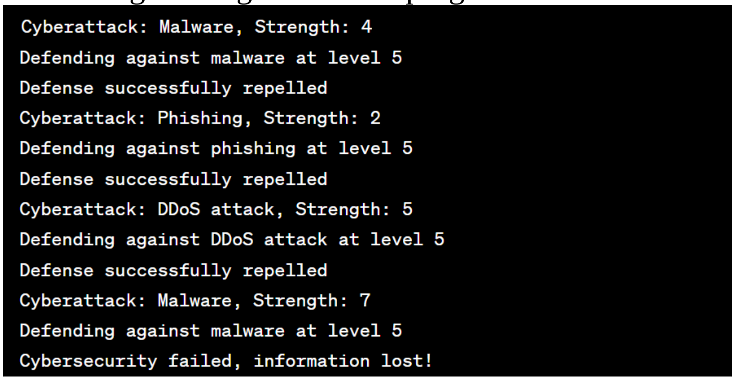
To demonstrate cybersecurity in armed conflicts, it is necessary to implement a simple programme that simulates the protection of military data from cyber-attacks. The main purpose of this programme is to simulate scenarios of cyber-attacks on military information systems and demonstrate measures to protect them.

```
import java.util.Random;
```

```
class MilitarySystem {
    private String data = “Secret information”;
    private String[] attacks = {“DDoS attack”, “Phishing”, “Malware”};
    private int securityLevel = 5;

    public void simulateAttack() {
        String attackType = attacks[new Random().nextInt(attacks.length)];
        int attackStrength = new Random().nextInt(10) + 1; // determining attack strength
from 1 to 10
        System.out.println(“Cyberattack:” + attackType + “, Strength:”  + attackStrength);
        // Simulating reaction to the cyberattack
        if (attackType.equals(“DDoS attack”)) {
            defendDDoS(attackStrength);
        } else if (attackType.equals(“Phishing”)) {
            defendPhishing(attackStrength);
        } else if (attackType.equals(“Malware”)) {
            defendMalware(attackStrength);
        }
    }

    private void defendDDoS(int strength) {
        System.out.println(“Defending against DDoS attack at level” + securityLevel);
        // Simulating actual defence intervention
        if (strength > securityLevel) {
            System.out.println(“Cybersecurity failed, information lost!”);
        } else {
            System.out.println(“Defence successfully repelled”);
        }
    }

    private void defendPhishing(int strength) {
        System.out.println(“Defending against phishing at level” + securityLevel);
        // Simulating actual defence intervention
        if (strength > securityLevel) {
            System.out.println(“Cybersecurity failed, information lost!”);
        } else {
            System.out.println(“Defence successfully repelled”);
        }
    }

    private void defendMalware(int strength) {
        System.out.println(“Defending against malware at level” + securityLevel);
        // Simulating actual defence intervention
        if (strength > securityLevel) {
            System.out.println(“Cybersecurity failed, information lost!”);
        } else {
            System.out.println(“Defence successfully repelled”);
        }
    }
    public void upgradeSecurity(int level) {
        System.out.println(“Increasing cybersecurity level by” + level);
        securityLevel += level;
    }
}

public class Main {
    public static void main(String[] args) {
        MilitarySystem system = new MilitarySystem();
        // Simulating cyberattacks
        for (int i = 0; i < 5; i++) {
            system.simulateAttack();
        }
        // Increasing cybersecurity level
        system.upgradeSecurity(2);
        // Simulating cyberattacks again
        for (int i = 0; i < 5; i++) {
            system.simulateAttack();
        }
    }
}
```

This code models a cybersecurity system in the context of military data. The main object is MilitarySystem, which has confidential data and a number of methods to protect against various types of cyber-attacks. As a result, a simulation of several cyber-attacks is displayed (Fig. 1). Type and strength are generated for each attack. The system protects against each attack depending on its type and strength. If the attack strength exceeds the level of cyber defence, the attack is considered successful and the information is lost. If the force is less than or equal to the level of cyber defence, the defence can be repelled.

Fig. 1. Fragment of the programme result



```
Cyberattack: Malware, Strength: 4
Defending against malware at level 5
Defense successfully repelled
Cyberattack: Phishing, Strength: 2
Defending against phishing at level 5
Defense successfully repelled
Cyberattack: DDoS attack, Strength: 5
Defending against DDoS attack at level 5
Defense successfully repelled
Cyberattack: Malware, Strength: 7
Defending against malware at level 5
Cybersecurity failed, information lost!
```

The programme itself is written in the Java programming language. At runtime, it displays information about the type and strength of the cyber-attack, and the result of protection against the attack. If the attack strength exceeds the level of cyber defence, a message about information loss is displayed. Otherwise, a message about successful protection is displayed. However, this programme is only a model for demonstrating the principles of cyber defence and response to cyber-attacks and does not represent a real cyber defence system.

3.3 Real-world examples of cyber-attacks on classified data during the war period and their comparative analysis

There are many cases of cyber-attacks on military or other information committed in different countries and in different years. For example, a cyber-attack on the Office of the General Staff of Ukraine in 2017, when Russian hackers attacked this office, which led to the loss of important military data and disruption of the command-and-control system. In 2008, hackers from China carried out a cyber-attack on the Pentagon’s computer network, as a result of which important military data was stolen. In 2015, Chinese hackers carried out a cyber-attack on the computers of the US Department of Defence, as a result of which military data was also stolen. In 2014, Russian hackers carried out a cyber-attack on the computers of the Ministry of Defence of Ukraine, as a result of which secret data was stolen and the military system was disrupted. In 2017, the Russian hacker group “Fancy Bear” carried out a cyber-attack on NATO computers, as a result of which important military information was stolen. There are many such examples, but the most relevant are cyber-attacks related to the full-scale invasion of Ukraine by the Russian Federation (RF) in 2022.

It is known that the Russian Federation launched a large-scale cyber campaign against Ukraine before the invasion in 2022. This campaign included phishing, DDoS attacks, and exploiting software vulnerabilities to steal sensitive information. Ukrainian cybersecurity experts have reported an increase in the number of cyber-attacks by Russia on Ukrainian government websites, energy and telecommunications sectors since the beginning of the invasion. It is obvious that the main objects of attention for attackers are five sectors: numerous private companies in the field of media and telecommunications, local governments, organisations of the security and defence sector, and government agencies. It is important to note targeted attacks, in particular, on the subcategory of local authorities that operate within the public sector.

Based on observations of the activity of Russian hackers, which includes constant attempts at espionage and implantation, it can be assumed that their main task, given by the military command, was to disclose the amount of information collected by Ukrainian law enforcement agencies. This information may include evidence, intelligence, and statements that may serve as the basis for criminal proceedings against spies, specific individuals, institutions, or organisations in the Russian Federation, with possible consequences in the form of sanctions or other measures. When collecting data, it can be noted that the main purpose is to obtain information about the current situation and cases that are being prepared for submission to the court, including data that has been transferred to certain law enforcement agencies as evidence for future arrests. Plans and evidence collected by Ukrainian law enforcement agencies for international judicial procedures are also an important element. Other criteria include a list of key witnesses and stakeholders for future trials of war criminals. It is also important to consider the lists of arrested persons and consider how to help them avoid responsibility and avoid transfer to the Russian Federation. Attention is drawn to personal identification data and information about persons against whom law enforcement officers submit applications to the court or prosecutor’s office for arrest or questioning. It also covers information about elite soldiers and officers who were captured during combat operations, and discussions about the possibility of exchanging them.

As of autumn 2023, Ukraine recorded almost 4,000 cyber-attacks from the Russian Federation. It is worth noting that cyber activity in the conflict between Russia and Ukraine is not limited exclusively to government participants. It is noted that non-state cyber actors on both sides of the conflict direct their actions to various organisations, including those operating in the financial services sector. This happens through relatively simple incidents known as DDoS. As an example, the pro-Russian hacker group “NoName057” threatened to attack the financial sector of Ukraine, which caused a large number of Ukrainian banks to undergo DDoS attacks. The most dangerous and capable organisations include the following: “Gamaredon”, “Sandworm”, and independent hacktivists.

Table 1 shows the activity of the defining participants in cyber-attacks on Ukrainian systems and their ability to perform a specific number of cyber operations during a certain time interval distributed over weeks. Each UAC-group can perform a limited number of operations and commit intrusions into internal networks. Maintaining access and recovery to compromised targets through embedded implants requires significant effort and resources from attackers.

Table 1: Detailed analysis of the activity of hacker groups

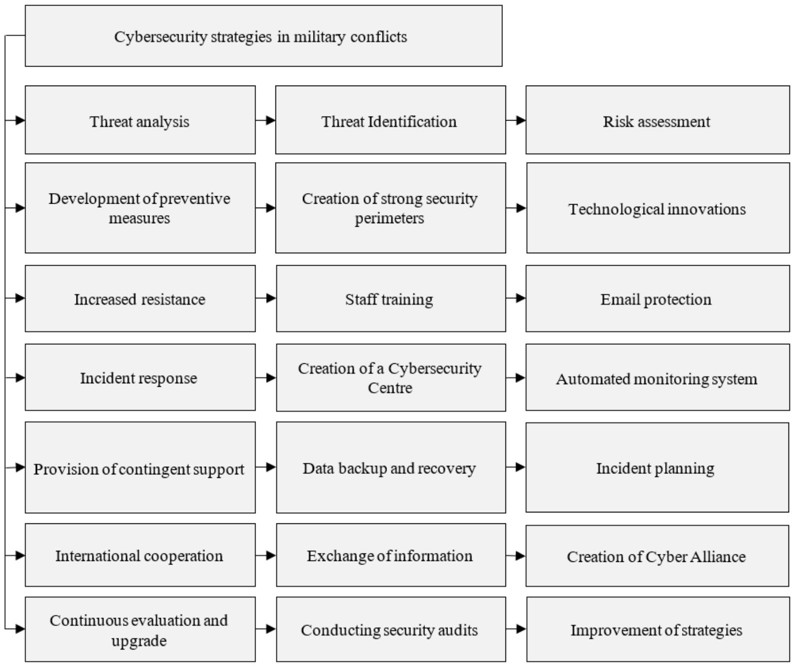
		January				February				March				April					May				June		
UAC-0028					2				2	1	4						1			3		6		2		2
UAC-0010	1	4	3	4		4	4	8	7	2	1		1	8	6	2	2	3	7	7	10	7		4	3	4
UAC-0041									1				1	1							1			1		
UAC-0082	1		1	2			2						1	1	1					3	1			1		1
UAC-0156														1	1											
UAC-0024															1				1							
UAC-1045															3	1										
UAC-0107					5						1											1			1	
UAC-0114					1																					
UAC-0100				1	2			2		1	3															
UAC-0056					1	1		18	3	2																
UAC-0150		1			2	1					2	1		1							1	1			5	1
UAC-0050						1	12	10										1								
UAC-0006																		1	11	1		5				1
UAC-1037												1				1	1									
UAC-0153												1														
UAC-0151												1														
UAC-0109								4				26					1	10								
UAC-0099														1				1			1					
UAC-0166																		1								
UAC-0135	1						1																1			

After analysing the changes over a certain period of time after a full-scale invasion, it is possible to draw conclusions about the frequency of operations, target planning, limited choice of strategic goals, opportunistic approach and the principle of “victim”, and security measures. In other words, for the most part, such hacker groups perform an average of one operation per month, although performance can vary significantly depending on the size and composition of the team. Usually, when exposed, the group needs time to move on to a new “victim”. Groups with a large number of participants usually spend about a month infiltrating and securing, while smaller groups may take 2-3 months to fully penetrate. In addition, the number of really important targets for cyber-attacks in support of military operations is limited, so after exposure, attackers often try to regain access or find alternative ways to invade. Attackers, with a large number of potential targets, resort to an opportunistic “victim” approach through related organisations and vendors. As for critical security measures, they include blocking certain types of executable files on all devices in the organisation, which makes it easier to protect against the implementation of many threats. Thus, these conclusions indicate the need to improve security measures and counter cyber threats to effectively protect against potential attacks. For this reason, it is recommended to develop specific cybersecurity strategies.

3.4 Development of cybersecurity strategies in armed disputes

The development of digital security strategies in the context of armed conflicts provides for a comprehensive approach to the protection of important military, diplomatic, and other information resources. The development of preventive measures will involve the introduction of technical and technological innovations to create reliable security perimeters. Incident response may also include the formation of a cybersecurity centre and the use of automated monitoring systems. Contingent provision will include systematic data backup and recovery. International cooperation can be manifested by the exchange of information and participation in international cyber alliances. The overall approach should be flexible and adaptive, providing full protection in high-risk conditions of armed conflicts (Fig. 2).

Fig. 2. Block diagram of cybersecurity strategies in military conflicts


Cybersecurity strategies in military conflicts
Threat analysis
Threat Identification
Risk assessment
Development of preventive measures
Creation of strong security perimeters
Technological innovations
Increased resistance
Staff training
Email protection
Incident response
Creation of a Cybersecurity Centre
Automated monitoring system
Provision of contingent support
Data backup and recovery
Incident planning
International cooperation
Exchange of information
Creation of Cyber Alliance
Continuous evaluation and upgrade
Conducting security audits
Improvement of strategies

An important element of digital security strategies is also the systematic verification and updating of measures in accordance with the latest technological and cyber measures. It is essential to consider the use of artificial intelligence and analytics to predict potential threats and prevent them in advance. It is worth focusing on building a cybersecurity culture within the organisation, which includes training personnel and forming a responsible attitude to cyber activities. Strategies need to be regularly adapted to changes in cyber threats, the geopolitical environment, and the rapid development of technologies to ensure an effective and high level of information protection in modern conditions of armed conflicts.

3.5 Summary and general recommendations. Investigation and comparison of scientific research

Summing up the research on information security in armed conflicts, it is possible to identify key aspects that affect the effectiveness of cybersecurity measures in war conditions. Software implementation and visualisation of attacks on military data revealed the various threats faced by military structures, and the importance of detecting and countering them to ensure the reliability of defence systems. Real-world examples of cyber-attacks on classified data during the war period highlighted the serious impact of cyber threats on important information resources. The Russian invasion of Ukraine in 2022 is a prime example of a large-scale cyber campaign and calls for improved security measures.

The development of cybersecurity strategies in armed conflicts includes a comprehensive approach that must necessarily consider threat analysis, preventive measures, increased resistance, incident response, contingent provision, international cooperation, continuous assessment and updating [11, 12]. A flexible and adaptive approach that covers all aspects of cybersecurity determines the success of protection in high-risk situations of armed conflict. General recommendations include improving technological security tools, implementing forecasting and prevention systems, training workers, building an information security culture, systematically updating and adapting to changes in threats and the technological environment.

For a more in-depth analysis of the topic of cybersecurity in the context of military conflicts, it is worth considering other studies in this area. For example, Mikiashvili explored various aspects related to information warfare and cyber warfare in the context of the military conflict between Russia and Ukraine, and in the framework of China-Taiwan relations [13]. The researcher reviewed the concept of information warfare (IW), which, unlike cyber warfare, is aimed at attacking computers, software, and control systems. He defined that information warfare involves the use of combat space and the management of information and communication technologies (ICTs) to achieve the goals set. The researcher also considered that information warfare involves manipulating information that the target object considers reliable, unnoticed by it, to make decisions that contradict its interests, but are beneficial for the person who initiates the information war. In addition, the researcher noted that the boundaries of the beginning and end of information warfare, its power or destructiveness, are ambiguous. As in this study, the above one deals with information warfare. However, this paper examines the methods of information security and protection against cyber-attacks during military conflicts, while the second paper examines information warfare itself and compares the concepts of IP and ICT.

Singh et al. examined the impact of stress on personal and professional qualities in various information professions [14]. The researchers stressed that cybersecurity professionals work in an ever-changing hostile threat environment and must comply with ever-changing industry requirements. Such a stressful environment can be compared to the conditions of war. The study provides a literature review aimed at identifying gaps and trends in the current literature on stress in the general workplace. In addition, possible promising areas for future research aimed at studying stress among cybersecurity specialists are highlighted. That is, both studies focus on the work of specialists in the field of information security in stressful conditions. However, this study focuses specifically on cybersecurity during martial law, and the other one – during any stressful factors that may not necessarily be related to war.

In turn, Thøgersen examined the impact of virtual groups on the occurrence of armed conflicts and thus the application of international humanitarian law (IHL) [15]. The researcher stressed that with the emergence of non-state actors as key participants in cyberspace and with the growing use of cyber operations in conflicts, regulating the actions of non-state actors in armed conflicts is becoming a hot topic. The application of provisions that lead to the application of IHL implies a certain level of organisation of non-state groups, which does not always correspond to the reality of virtual groups. To determine the possibility of rethinking the requirements for an organisation to better adapt to potentially diverse structures of virtual groups, the paper analyses the legal basis of requirements for an organisation and defines basic principles. Therefore, the general aspects of research are that they look at cyber operations in armed conflicts. However, the aforementioned study focuses on cyberspace rather than cyber defence, unlike this paper.

Stanciu et al. stressed that international cooperation and information exchange between countries is the main aspect of modern diplomacy, including climate diplomacy [16]. Much of the communication on this topic is based on digital technologies, so there is a risk of various cyber threats that can cause serious problems between partners, and lead to armed conflicts. The researchers noted that at the level of dialogue partners, joint activities to exchange best practices, information on cyber threats and initiatives to improve cybersecurity will contribute to strengthening the global framework for international cooperation and climate diplomacy. The purpose of the study was to identify a conceptual framework within which international collaborative efforts could improve collective resilience to cyber threats directed at information flows within the framework of digital climate diplomacy. It can be concluded that both studies focus on the emergence of cyber threats, including in armed conflicts. However, if this study focuses on the prevention of cyber threats during armed conflicts, then another is on the emergence of information threats from the standpoint of climate diplomacy.

The purpose of the study by Mohee was to assess the overall impact of cyber warfare between Israel and Iran on the security of the Arab region, using the concept of a regional security complex from Busan, Wever, and De Wilde [17]. To achieve this goal, the researcher analysed international relations in the Arab region, covering changes in the patterns of friendship and hostility, mutual dependence in security, and the distribution of forces. The study confirmed that the cyber war between these countries significantly affected the security of the Arab region. The consequences, risks, and threats of this cyber war have caused fundamental changes in the patterns of international relations in the Arab region, including increased mutual cybersecurity dependence, patterns of friendship and hostility, and the balance of cyber forces among the countries of the region. Thus, both studies look at cybersecurity in times of war. However, this study focuses on current information wars in general, paying special attention to cybersecurity during the war between the Russian Federation and Ukraine. And the second study focuses specifically on the digital war between certain Arab countries.

Khanam et al. considered technologies and partnerships in cutting-edge cybersecurity initiatives for the energy sector [18]. They stressed that the growing vulnerability to disclosure in the electricity sector requires attention, and cybersecurity strategies in various regions of the world recognise the need for joint research and the creation of a sustainable ecosystem with partners from industrial supply chains, academies, and states. Active cybersecurity in the energy sector includes identifying, protecting, and detecting potential threats [19]. In identifying the cutting-edge cybersecurity landscape in the electric power industry, the analysis considered the most effective cybersecurity technologies related to electricity, network management, and automation. In other words, both studies are looking at ways of cybersecurity. However, this study focuses on cybersecurity in armed conflicts.

Bartnicki et al. focused attention on information warfare, which is a new aspect in modern military conflicts [20]. The researchers noted that Russia’s attempts to distort events during the 2022 war were successfully resisted by Ukraine. The Russian Federation not only lost in the war for information, but also lost the support of the world community. Ukraine’s success in the field of information warfare has complex reasons, including Russia’s disregard for information warfare at the initial stage, the rapid response of Western countries to the ban on access to Russian information channels, and the position of President Volodymyr Zelenskyi. Social networks and unauthorised actions of Ukrainian citizens played an important role in shaping the perception of information about the war. The purpose of this study was to reveal the place of information warfare in the Russian military doctrine, the main phases, strategies, and goals of the conflict in the infosphere and cyberspace. In addition, the study highlighted the reasons for Ukraine’s success in this area, and the military and political consequences of Kyiv’s establishment of an information narrative of war. As a conclusion, both studies consider the information war between Ukraine and the Russian Federation. However, this study focuses specifically on cybersecurity techniques during this war, while the other focuses on a general analysis of information warfare.

Huda and Al-Fadhat analysed cybersecurity relations between China and the United States under the Trump administration [21]. They investigated changes in U.S. cybersecurity policy in 2019, when the government adopted a protective approach to ban the use of Chinese software and hardware in the United States. The researchers also looked at how the decision sparked a trade war between the two countries, and how the move was driven by U.S. business interests and security concerns. Using a political-economic approach to cybersecurity, the study argues that defensive policies were aimed at protecting the interests of American businesses and providing security for global technological transformation and economic stability. However, this strategy has led to an increase in trade disputes, especially in the areas of technology and processing large amounts of data. Thus, common aspects between papers are to analyse cybersecurity during certain conflicts. However, this study examines cybersecurity during modern armed conflicts, in particular, between Ukraine and Russia. And in the second – during the trade war between the United States and China.

Duneva considered communication technologies and malicious digital tools [22]. The main purpose of her research was to identify and analyse the impact of military events in Ukraine on business communications in the country and on cybersecurity. The purpose of the study was to highlight the impact of the use of communication channels, social networks, and the spread of misinformation. Data from various sources, such as mass media, newspapers, magazines, as well as studies and briefings related to Ukraine, were used for the analysis. As in this study, the above focuses on the impact of technology on the war in Ukraine. However, this paper examines methods of providing protection against Information threats during war, and the other – analysis of the impact of digital tools on war.

Iova and Watashiba investigated the prevalence of ICT and the rise of cyber threats, prompting countries to consider cybersecurity nationally and develop appropriate strategies [23]. The researchers emphasised that although these strategies have a similar terminology framework, they are adapted to national contexts and differ by region, culture, and political environment. They also examined all countries that published national cybersecurity strategies to determine their positions on war, neutrality, and international cooperation. The hypothesis was that international cooperation is present in most strategies, but they may not sufficiently address armed conflict and neutrality at all. The results of the study represent a global case study that can point to ways to improve and strengthen democratic coalitions. In other words, the common thread between the two papers is the development of cybersecurity strategies and the attitude of certain countries to war. However, this study focuses on strategies to protect against cyber-attacks during the war, and the other – on these strategies in general.

In turn, the study by Qandeel aims to identify the link between agent-related technology and environmental protection during armed conflicts by exploring how agent-based modelling and simulation can be used to provide environmental protection [24]. The paper discusses in detail the principle of caution and proper treatment as appropriate rules, and explains the legal benefits of using ABMS to protect and preserve the natural environment. The researcher argues that the implementation of ABMS helps states better understand the environmental consequences of conflicts, rethink their military activities, and comply with recognised rules and regulations. It should be concluded that both papers work focus on the use of technology during armed conflicts. However, this study considers specifically cybersecurity methods, while the other examines modelling and simulation technologies.

Martínez et al. emphasised that over the past decades, cybersecurity research has focused on the importance of developing cyber defence capabilities for both industrial and military, and for corporate and public sectors [25]. Despite the introduction of policy measures to promote interaction in the field of protection, threats in cyberspace continue to grow and affect various organisations, regardless of their size. Researchers review existing principles, policies, and conditions in the international context of cybersecurity in the military and marine environment and determine how these principles are applied through specific measures to the environment of naval units. Thus, both studies consider cybersecurity, including for the military sector. However, unlike this study, the above study also considers digital security for the marine sector.

Researchers [26] examined the impact of the use of commercial satellites in military operations on the Department of Defence's (DD) need for a supply chain concept to address cyber threats in space. The researchers proposed a cybersecurity supply chain (CSC) framework designed to provide a comprehensive approach to protecting commercial satellites used by the DD and their components. This strategic approach, improved with the requirements of the National Institute of Standards and Technology (NIST) and the upcoming cybersecurity maturity model certification process (CMCP), simplifies NIST requirements for small businesses and extends them to commercial vendors. The CSC framework complements the CMCP process by taking into account the cybersecurity requirements for all subcontractors supporting a commercial space asset, and also includes an assessment similar to the CMCP, which provides points to subcontractors for compliance with cybersecurity requirements. Similar to this study, the above focuses on cybersecurity strategies in military operations. However, if this study focuses specifically on cybersecurity in military conflicts, then the other one – on cybersecurity using satellites.

Like previous researchers, [27] also considered the concept of cyberwarfare. They stressed that this new form of conflict harms not only the military, but also affects all areas of human life. As cybersecurity has become a critical element of military operations, the military community is highly dependent on the private sector to ensure the cybersecurity of missions. However, this can increase the risk of mission disruption or failure due to military secrecy. In order to solve this problem, a special cybersecurity training system was built for internal use. The researchers proposed a scripted, interactive, and immersive cybersecurity learning platform that comprehensively supports a variety of learning functions. Through the demonstration of the prototype, the researchers confirmed the possibility of effective and realistic cybersecurity training, which is used not only in the military, but also in the private sector. In other words, both studies consider information warfare and ways to protect against cyber threats. However, this study develops cyber defence strategies under military conditions, while the rest develops a cybersecurity training platform [28].

Summarising the results of the analysis of various papers, certain conclusions can be drawn. For example, information wars are an integral part of modern conflicts, and cybersecurity is an important part of military operations. Developing effective strategies is critical to protecting military systems, and international cooperation and the development of common standards is an important element of national cybersecurity strategies. In addition, the private sector plays a key role in ensuring cybersecurity, especially in the context of cyber warfare, and the development of effective cybersecurity training systems can significantly increase the readiness of the military for cyber-attacks.

4 Conclusion

In this study, certain cybersecurity strategies were developed in the context of current military conflicts, and methods of analysis, experiment, and generalisation were used to achieve this goal. As a result of applying the analysis method, key aspects of armed conflicts and cyber threats were thoroughly investigated, and other studies on this topic were analysed. The analysis of information warfare in different geopolitical contexts pointed to the diversity of threats and determined the impact of cyber-attacks on different sectors of society. Consideration of the concepts of information warfare and cyber warfare determined their interaction and impact on security in the context of military conflicts. In general, the method of analysis turned out to be a tool that opens up versatility and relationships in the context of active modern conflicts, contributing to a deeper understanding of the situation and identifying the main factors and causal relationships.

The experimental method was used to test the practical effectiveness of the developed strategies. The implementation of the programme to simulate the protection of military information from cyber-attacks highlighted the need for flexible and adaptive measures in the fight against real threats. The established block diagram of information security strategies in armed conflicts provided a clear picture of the interaction of key components and helped identify weaknesses for further improvements. And the developed table of comparison and analysis of the activity of certain hacker organisations allowed objectively assessing the risks and threat level, which created the basis for strategic planning of cybersecurity measures. Thus, the coordinated activity of this method helped not only to evaluate the effectiveness of strategies, but also to identify and correct problematic aspects in the field of cybersecurity. The generalisation method allowed drawing general conclusions and recommendations. The synthesis of the data obtained determined that effective cybersecurity strategies include a comprehensive approach, including threat analysis, preventive measures, increased resistance, incident response, and international cooperation.

General recommendations include improving technical protection tools, implementing forecasting and prevention systems, training specialists, and constantly updating strategies to respond more effectively to changes in threats and the technology environment. The recommendations also include organisational aspects, such as setting up cyber defence centres and ensuring a cybersecurity culture among staff. It is worth emphasising the importance of international cooperation and the development of a regulatory framework to create a common front in the fight against cyber threats. This integrated approach will contribute not only to an effective response to existing threats, but also to readiness to meet future cybersecurity challenges.

This study opens the way for further scientific research in the field of cybersecurity in the context of military conflicts, in particular, improving simulation methods and developing adaptive strategies to combat the growing level of information threats. Moreover, in further papers, it is possible to consider the issues of effective management of cyber-attacks, the development of new technologies for predicting attacks, and the creation of integrated information security systems for various sectors of society.

ACKNOWLEDGEMENTS
None.

References

[1] Koval, V., Semenenko, O., Baranov, S., Ostrovskyi, S., Akinina, T., & Siechenev, O. (2023). The role and place of robotic systems in modern wars and armed conflicts: Theoretical aspect. *Journal of Scientific Papers Social development & Security, 13*(5), 256-276.

[2] Boychenko, O., Uminskyi, V., & Krymets, B. (2022). Improving the public key infrastructure of the Armed Forces of Ukraine. *Science and Defence, 2.* https://doi.org/10.33099/2618-1614-2022-19-2-51-55

[3] Bohomia, V. I., & Kochegarov, V. S. (2023). Cybersecurity in cloud services using cryptographic methods. *Water Transport*, *37*(1), 239-246.

[4] Apakhayev, N., Madiyarova, A. S., Aigarinova, G., Ryskaliyev, D. U., Buribayev, Y. A., & Khamzina, Z.A. (2017). Current trends of legal regulation of relationships in the social protection sphere. *Man in India, 97*(11), 221-231.

[5] Ternovyy, O., Shkurenko, O., & Minenko, L. (2023). Problematic aspects of cyber defence: Place and role of cyber defence in the Armed Forces of Ukraine. *Modern Information Technologies in the Sphere of Security and Defence*, *46*(1), 23-31.

[6] Ostrovskyi, S. O. (2022). Legal status of military communications and cyber security in the system of the armed forces of Ukraine. *Kyiv Journal of Law*, *3*, 86-91.

[7] Zhyvylo, Y., & Dokil, V. (2023). Model of assessment of military communication and cyber security capabilities of the Armed Forces of Ukraine for performing tasks of reflecting military aggression in cyber space. *Modern Information Technologies in the Sphere of Security and Defence*, *46*(1), 32-39.

[8] Vilks, A., Kipane, A., Kudeikina, I., Palkova, K., & Grasis, J. (2022). Criminological Aspects of Current Cyber Security. *Revista de Direito, Estado e Telecomunicacoes*, *14*(2), 94-108.

[9] Boyd-Barrett, O. (2023). Media and cultural agenda in the EU countries against the background of russian military aggression in Ukraine (sociological and contextual research). *European Chronicle, 8*(1), 37-45.

[10] Karamyshev, D., Suvorov, V., Didok, Y., Sobol, R., & Myrna, N. (2024). Multi-level public administration in the context of hybrid threats. *Social and Legal Studios*, *7*(2), 44-54.

[11] Kanybekova, B., Arstanbekov, M., Kakeshov, B., Erdolatov, C., & Artykbaev, I. (2023). Criminological Aspects of the Behaviour of Victims of Cyberattacks: Case Analysis of Hacking State Organisations Ensuring National Security. *Pakistan Journal of Criminology*, *15*(4), 175-192.

[12] Vilks, A., Kipane, A., & Krivins, A. (2024). Preventing international threats in the context of improving the legal framework for national and regional security. *Social and Legal Studios*, *7*(1), 97-105.

[13] Mikiashvili, S. (2023). Information war as a result of the information-technological revolution. https://www.igi-global.com/gateway/chapter/332280#pnlRecommendationForm

[14] Singh, T., Johnston, A., D'Arcy, J., & Harms, P. (2023). Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(2), 100-126.

[15] Thøgersen, M. (2023). Virtual groups and the triggering of armed conflicts. *Nordic Journal of International Law*, *92*(3), 329-348.

[16] Stanciu, A., Topor, S., & Ciuperca, E. (2023). Strengthening resilience in digital climate diplomacy: A cybersecurity perspective. *International Journal of Cyber Diplomacy*, *4*, 77-88.

[17] Mohee, A. (2023). The impact of the Israeli-Iranian cyberwar on Arab regional security. *APSA Preprints*, *1*. https://doi.org/10.33774/apsa-2023-1vd97

[18] Khanam, M., Garces, E., Daim, T., & Alsoubaie, F. (2023). Technology domain analysis: Ecosystem for proactive cybersecurity in the energy sector. In *Cybersecurity* (pp. 267-295). Springer.

[19] Quraishi, A., Rusho, M.A., Prasad, A., Keshta, I., Rivera, R., & Bhatt, M.W. (2024). Employing Deep Neural Networks for Real-Time Anomaly Detection and Mitigation in IoT-Based Smart Grid Cybersecurity Systems. In *3rd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2024*. Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ICDCECE60827.2024.10548160

[20] Bartnicki, A., Kużelewska, E., & Ożóg, M. (2023). Information and information technologies in the 2022 Russian-Ukrainian war. In *War in Ukraine. Media and Emotions* (pp. 21-41). Palgrave Macmillan.

[21] Huda, M., & Al-Fadhat, F. (2022). The political economy of the US-China cybersecurity relations and trade war under the Trump administration. *Journal of Islamic World and Politics*, *6*(2), 188-206.

[22] Duneva, E. (2023). The impact of the war in Ukraine on cybersecurity. In *Proceedings of the 1st International Scientific and Practical Conference "Modern Knowledge: Research and Discoveries"* (pp. 35-40). InterConf.

[23] Iova, R. A. S., & Watashiba, T. (2023). NCSS: A global census of national positions on conflict, neutrality and cooperation. In *Proceedings of the 22nd European Conference on Cyber Warfare and Security* (pp. 420-428). Academic Conferences International Limited.

[24] Qandeel, M. (2023). The protection of the natural environment in armed conflicts and agent-based modelling. *International Review of the Red Cross*, *1*. https://doi.org/10.1017/S1816383123000528

[25] Martínez, F., Guevara, F., Sánchez, L.E., & Santos-Olmo, A. (2023). Cybersecurity: A general framework in the maritime and military world. *Ciencia y Tecnología De Buques*, *17*(33), 51-60.

[26] Fleming, C., Reith, M., & Henry, W. (2023). Securing commercial satellites for military operations: A cybersecurity supply chain framework. *Proceedings of the 18th International Conference on Cyber Warfare and Security*, *18*(1), 85-92.

[27] Lee, D., Kim, D., Lee, C., Ahn, M., & Lee, W. (2022). ICSTASY: An integrated cybersecurity training system for military personnel. *IEEE Access*, *10*, 62232-62246.

[28] Russian cyber operations. 2023. https://cip.gov.ua/ua/news/the-amount-of-information-operations-with-the-cyber-component-has-grown