MULTIDISCIPLINARY SCIENCE JOURNAL

REVIEW ARTICLE
Published Online: January 21, 2024
https://doi.org/10.31893/multiscience.2024ss0219

Special Issue: Modern Changes in Education, Labor Market, and Development

Cybersecurity in the face of information warfare and cyberattacks

Olena Kravchenko[a] ✉ | **Vladyslav Veklych**[b] | **Mykhailo Krykhivskyi**[c] | **Tetiana Madryha**[d]

[a]Science Laboratory, The National Academy of Security Service of Ukraine, Kyiv, Ukraine.
[b]Interregional Academy of Personnel Management, Kyiv, Ukraine.
[c]Department of Software Engineering, Institute of Information Technologies, Ivano-Frankivsk National Technical University of Oil and Gas, Ivano-Frankivsk, Ukraine.
[d]Department of Political Institutes and Processes, Faculty of History, Politology and International Relations, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine.

Abstract Cybersecurity in the face of information warfare and cyberattacks in the modern world is one of the most critical issues of our time. Driven by the rapid development of technologies and digital transformation, threats to information security are becoming even more severe. Nowadays, almost every aspect of our lives, from personal data to critical infrastructure systems, is affected by cyberattacks. Information warfare has become a complex struggle where digital battles are integral to modern conflict. Countries, corporations, and even criminals fight for control over data and influence over critical systems. All this creates a situation where a defense against cyber threats is a top priority. The article aims to provide a detailed analysis and understanding of cyber threats' dynamics in the context of information warfare. It also highlights effective strategies and measures to ensure cybersecurity in such a challenging environment. The research methodology is based on comparing and analyzing information on real cyberattacks, studying the vulnerabilities of information systems, and developing strategies and technologies to counter cyber threats. The study employs both quantitative and qualitative methods, including statistical analysis and case studies. The results of the study revealed the main features of information warfare and their impact on cybersecurity globally and within specific organizations and states. Conflicting parties can use digital means to attack opponents, destroy their critical infrastructure, obtain secret information, or disrupt their operations. Information operations may use phishing and social engineering tactics to access essential resources or information. The organizations and states that find themselves at the epicenter of information warfare must carefully ensure the cybersecurity of their information resources.

Keywords: countering cyber criminals, cyber security, information security, information war, monitoring of cyber threats, protection of information systems.

1. Introduction

Over more than two decades, the Internet has played a crucial role in global communication and has become an integral part of people's lives worldwide. Innovations and accessibility in this field have significantly increased the number of Internet users, with approximately 3 billion people using this resource today (Tavolato et al., 2021).

The Internet has created an extensive global network, contributing billions of dollars to the world economy annually (Al-Ghamdi, 2021). Currently, most economic, commercial, cultural, social, and governmental activities at global and regional levels, including people, nonprofit organizations, and government institutions, occur in cyberspace (Aghajani & Ghadimi, 2018). Critical and sensitive infrastructure and systems either exist within cyberspace or are controlled, managed, and operated through it. Most confidential information is transmitted to or based in this space (Akhavan-Hejazi & Mohsenian-Rad, 2018). Media activities also take place in cyberspace, and most financial transactions are conducted through it (Bullock et al., 2021).

Revenues from the cyberspace sector have significantly increased, and cyberspace indicators have become a vital component for measuring this level of development. Many countries have invested substantial resources in cyberspace, and its impact has reflected on the material and spiritual growth of citizens (Amir & Givargis, 2020). Therefore, various aspects of citizens' lives are closely connected to cyberspace, and any instabilities and threats directly affect their lives (Cao et al., 2019).

Cyberspace has presented new security challenges for governments. The low cost of access, anonymity, and uncertainty of the origin of threats have created conditions for various actors, including organizations and people, to carry out cyberattacks and threats in general. There are various scenarios of significant incidents, including attacks on financial documentation, stock markets, and power plants (Dash et al., 2021).

Cyberspace has become a crucial aspect of the global economy and communication and national security for countries. Due to the large number of critical systems controlled through cyberspace and the transmission of confidential information through it, threats in this sphere have become increasingly severe.

Potential consequences of cyberattacks may include significant financial losses, disruption of critical infrastructure, and breaches of citizens' privacy and data confidentiality. These threats are not limited to a single country, as cyberspace has no clear borders, and attacks can be launched from anywhere in the world.

Effective protection of cyberspace and addressing cybersecurity issues have become essential tasks for countries and the international community in general. International standards and strategies must be developed to prevent cyberattacks, detect them, and respond to them. It is also crucial to establish legal frameworks and norms for cyberspace to ensure the rights and responsibilities of all entities in this global sphere. Therefore, our research is aimed at studying key threats and risks in the field of cybersecurity, developing strategies to overcome them, and establishing methods to enhance the protection of information systems at all levels.

2. Literature review

Cybersecurity is becoming increasingly important in the infrastructure of every country and organization. In the short term, a company actively working on cybersecurity can achieve a high status and exceptional results. This success directly depends on protecting confidential information from potential competitors, including customer personal data (Ji et al., 2021).

One of the key tasks for any company or organization is ensuring the highest level of cybersecurity. It involves practical measures to safeguard information, networks, information systems, and data from potential internal or external threats. Cybersecurity specialists aim to protect networks, servers, intranets, and computer systems, as well as provide access to this information only to authorized users (Karbasi & Farhadi, 2021).

Furthermore, understanding various types of cybersecurity is crucial for ensuring overall security. Figure 1 illustrates the types of cybersecurity for a better understanding of this concept.

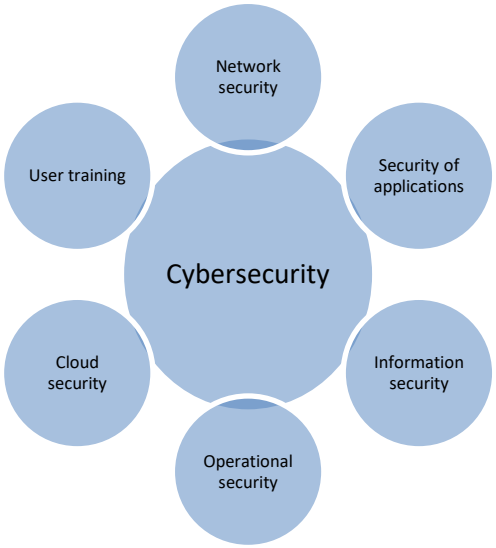

Figure 1 Types of cybersecurity.
Source: compiled by the authors.

1. Network security. It involves measures aimed at preventing interference, such as viruses or hacker attacks. Network security is a set of solutions that enable organizations to keep computer networks out of the reach of hackers, organized attackers, and harmful software (Zhang, 2021).
2. Security of applications. The use of hardware and software tools (such as antiviruses, encryption, and firewalls) is designed to protect the system from external threats that may affect application development (Alkatheiri et al., 2021).
3. Information security. Protection of physical and digital data from unauthorized access, disclosure, misuse, unlawful modification, and deletion (Ogbanufe, 2021).
4. Operational security. Processes and decision-making aimed at controlling and protecting data. For example, it may include setting up permissions for users to access the network or establishing procedures that determine when and where information data can be stored (Ogbanufe, 2021).
5. Cloud security. Cloud-based data protection (software-based) and monitoring to eliminate on-premises attack risks (Nguyen & Golman, 2021).
6. User training. It is aimed at those aspects of cybersecurity that may be unforeseen and related to people's actions. This means that user training is based on awareness of possible threats and actions to ensure online security, as anyone can

inadvertently introduce a virus into a security system. Teaching users how to delete suspicious email attachments and avoid connecting anonymous USB devices and other devices should be part of any company's corporate security plan (Qiu et al., 2021).

3. Methods

The article adopts a comprehensive approach to the study of essential aspects in the field of cybersecurity.

The literature review serves as the initial stage of the research and involves the analysis of existing literature and scientific sources related to cybersecurity, information warfare, cyberattacks, artificial intelligence (AI) technologies, and international cooperation in this field. This stage helps identify key concepts and issues that form the basis of the research.

Next, the research process includes the analysis of informational sources such as news, reports, statistics, and other information sources related to current cyber threats, cyberattacks, and information warfare. This analysis helps identify contemporary trends and examples in this field.

An analysis of specific incidents, attacks, and cyber operations that have occurred in real life is conducted to understand better the issues related to cybersecurity and information warfare. It allows for the examination of specific scenarios and their consequences.

After analyzing the informational sources and examples, theoretical and practical conclusions are drawn regarding the interplay between cybersecurity and information warfare, as well as the practical implications for society, the economy, and politics.

4. Results and discussion

Information warfare is a modern type of conflict in which clashes occur both on military battlefields, in cyberspace, and in the digital environment. This term includes various aspects, and the definition may vary depending on the context. The main features of information warfare are listed in Table 1.

Table 1 Features of information warfare.

Feature	Description	Example
Information operations	Information operations include actions aimed at the opponent's information sphere. They may include the spread of disinformation, propaganda, fake news, and influence on social networks and media.	Russia's information campaign during the war in Ukraine has used disinformation and propaganda to influence public opinion in Ukraine and abroad.
Target impact	Information warfare always has specific goals. These goals can have an impact on election results, destabilize society, undermine people's trust in the government, etc.	Russia's information campaign during the 2016 US election aimed to influence the vote and undermine confidence in American democracy.
Use of technologies	Information warfare uses modern technologies, including cyberattacks, social media manipulation, algorithmic dissemination of information, and other means.	The WannaCry cyberattack in 2017, which spread worldwide, was an example of using cyberweapons to harm information systems.
The role of states and unconventional actors	Information warfare can be waged both by state and non-state actors, such as terrorist or hacker groups.	The Anonymous hacker group carries out various types of information operations aimed at revealing corruption and other state issues.
Secrecy and concealment	Information warfare is often conducted using secret and covert methods, making detecting and countering such actions difficult.	Fake news can be spread anonymously through social media, making identifying the source of disinformation difficult.
Impact on the social structure	Information warfare can cause social changes, such as the division of society, public outrage, and undermining trust in the government.	The spread of religiously or racially hostile propaganda can contribute to societal conflicts and divisions.

Source: compiled by the authors.

Let us consider the impact and consequences of information warfare during the conflict in Syria.

Different sides used information warfare to achieve their political and military goals during this conflict. It is an important aspect, as information operations can influence public opinion, shape the international community's impression, and even influence military operations on the battlefield.

One specific example of the conflict in Syria is the situation with the photo of a boy named Alan Kurdi. In August 2015, this photo shocked the world community and became a symbol of war horror in Syria and its refugees. The picture showed the

body of a three-year-old boy, who was found on the beach after his family tried to cross the Mediterranean Sea to escape the military conflict.

This photo became a tool of information warfare in the context of the Syrian conflict. Different conflicting parties and political groups used it to influence public opinion and the international community. Some have used this photo to emphasize the need for humanitarian aid and refugee support. Meanwhile, others have used it to call for tougher measures in relations with the Syrian government and the Russian Federation (Yang et al., 2021).

This example illustrates how a photo has become a tool of information warfare, influencing public opinion and international response to the conflict.

The main components of the information war in Syria are shown in Figure 2. These components complemented each other and were interdependent.

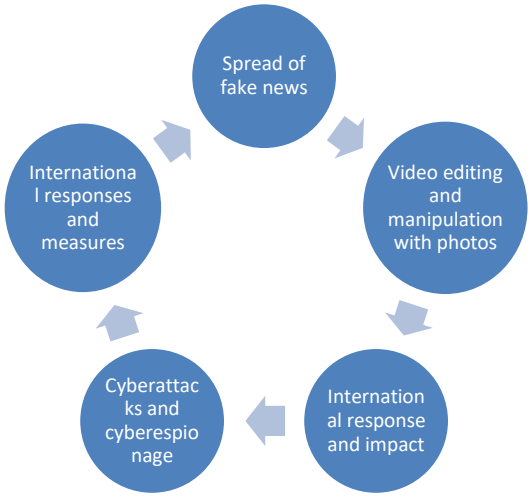

Figure 2 The main components of the information war in Syria.
Source: compiled by the authors.

1. *Spread of fake news.* One of the key strategies in information warfare is disseminating fake news or misinformation. It involves creating false messages spread through social media or other channels to influence public opinion and belief in certain events.

In 2017, there were reports of several incidents involving the use of chemical weapons in Syria. One of the most well-known incidents occurred in the city of Khan Sheikhoun, where it was alleged that the Syrian government used chlorine gas and sarin to attack the civilian population. This information spread through social media and other information channels, causing widespread international outrage.

However, it later turned out that this information was the subject of information warfare and was not substantiated. Some research and expertise indicated that the fake scenario was developed to discredit the Syrian government and provoke an international reaction against it. This example illustrates how the spread of fake news can be used to influence public opinion and global response in the context of the Syrian conflict (Levytska et al., 2022).

2. *Video editing and manipulation with photos.* Another tactic in information warfare is the use of video editing and photo manipulation to create images that can be offensive or provocative. This can trigger a reaction from the audience and deepen the conflict.

Indeed, in the Syrian conflict, there were cases of video editing and photo manipulation to create provocations and offensive images. For example, the dissemination of a fake video clip that created a false image of events on the battlefield.

In 2016, a video clip emerged showing the moment when children from the "White Helmets" group (an organization involved in humanitarian activities in Syria) met with children who survived an airstrike in the Syrian city of Aleppo. The video clip shocked the international community, causing widespread outrage and calls for international action against the Syrian government and its allies.

However, it was later revealed that this video clip was manipulated to create a negative image of the Syrian government and draw global attention to the conflict. This example illustrates how video editing and photo manipulation can influence public opinion and provoke outrage in the information war in Syria.

3. *International response and impact.* The information war in Syria also has global consequences. Public opinion in different countries and the response of international organizations have been significantly altered by information operations, which, in turn, affected the decisions of politicians and the diplomatic process.

In 2017, there were several chemical attacks in Syria, including an attack on the city of Khan Sheikhoun. Video materials and images showing the aftermath of these attacks were spread through social media and other information channels.

The global community and many countries were outraged by these horrific events, and international organizations such as the United Nations and the Organization for the Prohibition of Chemical Weapons (OPCW) paid attention to this information evidence. However, some of this news was later found to be fake and the subject of disputed investigations. In the world of information warfare, false information, especially in the context of conflicts, is used as a tool of manipulation or psychological warfare. It is essential to verify sources and confirm information before concluding.

4. *Cyberattacks and cyber espionage.* In addition to disinformation, information warfare includes cyberattacks and cyberespionage. Parties to a conflict may attempt to breach the computer systems of their opponents or obtain confidential information (Amir & Givargis, 2020).

In the Syrian conflict, there were numerous examples of cyberattacks and cyberespionage. One of the well-known examples is cyberattacks on various computer systems and infrastructure used by different sides of the conflict.

For instance, in one episode of the conflict, cyberattacks were recorded against the computer systems of an opposition group. These attacks aimed to steal confidential information, including plans and communications. These attacks targeted vulnerabilities in the opponent's cybersecurity and aimed to gain an advantage in the information space (Borodina et al., 2022).

There were also examples of cyberespionage, where parties to the conflict sought to obtain information about strategic objects and enemy movements through hacking computer systems or developing spyware.

These examples demonstrate how cyberattacks and cyber espionage have become integral parts of modern conflicts and information warfare, where parties use these methods to achieve their goals and gain an advantage in the information space.

5. *International responses and measures.* In response to the information warfare in Syria, various countries and international organizations have taken steps to detect disinformation, create counter-propaganda, and strengthen cybersecurity.

One example of international response to information warfare in Syria is the actions of individual countries and international organizations to identify disinformation and create counter-propaganda. Many Western countries developed and disseminated content that aimed to respond to fake news and misinformation spread by various sides of the conflict. This included creating fact-checking materials highlighting accurate information, debunking myths, and spreading false claims.

International organizations and initiatives also aimed at strengthening cybersecurity and protection against cyberattacks in information warfare. These measures and initiatives illustrate that the international community understands the importance of combating information warfare and its consequences in the Syrian conflict.

Let us consider each aspect of the impact of information warfare on cybersecurity more closely based on the data on the conflict in Syria, which is given in Table 2.

Table 2 Aspects of information warfare impact on cybersecurity.

Aspect	Description	Example
Cyberattacks and cyber espionage	In the Syrian conflict, cyberattacks are being used by various stakeholders to harm opponents' computer systems. It may include attempts to hack into systems to gain access to secret information or affect the operations of vital facilities.	In 2015, the APT28 hacker group (linked to Russian intelligence services) organized cyberattacks on Ukrainian military facilities during the conflict in eastern Ukraine. These attacks were aimed at gathering information and influencing critical military processes.
Fake news and disinformation	The spread of fake news and disinformation has become a common practice during the Syrian information war. Bots created false messages that were disseminated through social media or other channels to influence public opinion and perception of events and create stereotypes.	Since 2014, Russian bot forms have been spreading fakes about the Ukrainian army shelling Donbas, deliberately killing civilians.
Protection against cyber threats	Cybersecurity is becoming increasingly important in the context of information warfare. Countries and organizations need to develop and implement cybersecurity strategies to protect against cyberattacks and preserve confidential information. Cyberdefense infrastructure and cybersecurity training are essential.	The Syrian government has stepped up cybersecurity measures to protect its critical facilities from cyberattacks and has been working to improve cybersecurity within the conflict.
International responses and measures	Various countries and international organizations have taken steps to identify disinformation, create counter-propaganda, and strengthen their cybersecurity.	In 2017, Canada established a special expert group to examine disinformation emanating from different conflict parties in Syria. This group provided analytical reports and recommendations on measures to counter disinformation.

Source: compiled by the authors.

These aspects demonstrate how the information war in Syria affects cybersecurity and requires comprehensive measures to protect infrastructure and information resources in a conflict.

Cyberattacks are specially planned actions that are carried out to hack, destroy, or illegally access computer systems, networks, and devices. Cyberattacks can be of different types and aimed at other targets. The main types of cyberattacks are shown in Figure 3.

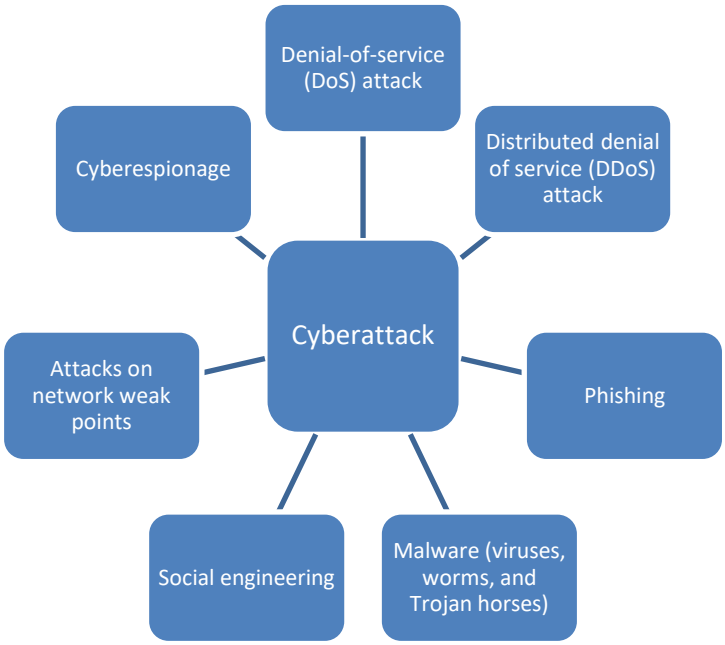

Figure 3 The main types of cyberattacks.
Source: compiled by the authors.

1. Denial-of-service (DoS) attack. During such an attack, hackers try to overload the system, forcing it to refuse to serve legitimate users. It may lead to the inaccessibility of the website or other online resources.

2. Distributed denial of service (DDoS) attack. In this case, many computers that are usually part of a botnet send requests to the target server simultaneously, which overloads it and makes it unavailable.

3. Phishing. These attacks involve hackers impersonating authorized users or organizations to obtain confidential information, such as passwords or bank details.

4. Malware (viruses, worms, and Trojan horses). Attackers use the software to access the system or steal its data illegally.

5. Social engineering. Criminals manipulate people to gain access to confidential information. For example, fraudsters can call company employees posing as information support and ask for passwords.

6. Attacks on network weak points (e.g., programs or equipment are not sufficiently updated). Hackers can exploit this vulnerability to break into systems.

7. Cyberespionage. Attacks on systems to gather information. This can be an important element of cyber intelligence and cyberwarfare activities.

Cyberattacks are becoming increasingly dangerous as modern technologies provide criminals more opportunities and anonymity. In this regard, protecting against cyberattacks is becoming a vital task for corporations, governments, and citizens.

The real SolarWinds incident, also known as SolarWinds or SUNBURST, occurred in December 2020. It was a cybersecurity breach that posed a serious threat to thousands of companies and government institutions.

The attackers stole access to the network of SolarWinds, a company that specializes in developing network monitoring software. They exploited a security flaw in the company's well-known software product called Orion and made changes to the Orion software update. Companies that use SolarWinds Orion downloaded this probe update without realizing that it contained malware code.

After infiltrating customer networks, the attackers accessed sensitive data, including email, documents, and other information. Furthermore, they used the access to infrastructures to identify government agencies and large companies that they could potentially use for attacks or to steal confidential data.

This cyberattack resulted in a significant loss of confidential information, including documents, correspondence, and other information. SolarWinds experienced financial losses and reputational damage as a result of this incident.

The 2007 cyberattack on Estonia was one of the most famous cyberattacks in the country. It was launched in response to the demolition of a public monument to a Soviet Union soldier from the central square in Tallinn. This caused protests and outrage among the Russian-speaking population in Estonia. The cyberattack included large-scale DDoS attacks on key

infrastructure facilities, including banks, government websites, and other information systems. The hackers massively requested access to these systems, overloading them and making them inaccessible to users. The attack also targeted media and telecommunications companies. This resulted in the interruption of communications and made it impossible to access independent sources of information (Kryshtanovych et al., 2021). At the same time, disinformation was spread through social media and the Internet, which led to increased tension and conflict between the Estonian and Russian communities in the country.

The cyberattack caused severe technical damage, including the inaccessibility of information systems and financial losses for companies and government agencies. The massive volume of attacks and cyber-attacks emphasized the threat to state infrastructure and national security. The cyberattack on Estonia attracted the international community's attention and expressed serious concerns about cyber threats and the need to improve cybersecurity.

Cyberattacks can have serious consequences for the society and economy of a country or organization. A detailed analysis of these consequences is presented in Table 3.

Table 3 Consequences of cyberattacks.

Consequence	Description
Economic losses	Cyberattacks can lead to huge economic losses. For example, the loss of access to information systems, theft of confidential information, or the interruption of operations can have a significant impact on the financial situation of companies and government budgets.
Loss of trust in technologies	After cyberattacks, citizens and companies may lose confidence in technologies and the Internet, which may affect the development of the digital society.
Legal cases and reputational losses	Cyberattacks can result in legal cases, which can lead to high expenses in resolving legal issues. In addition, reputational losses can affect the business reputation of organizations and countries.
National security threats	Cyberattacks can be used to hack into government systems and national defense systems, jeopardizing national security.
Violation of privacy	Cyberattacks can lead to a violation of citizens' and customers' privacy, as attackers can gain access to personal information and confidential data.
Security violations	Cyberattacks can pose a threat to the physical security of citizens, especially if they involve critical infrastructure facilities such as power plants or transportation systems.
Social consequences	Cyberattacks can cause social tensions and conflicts, especially if they target nationally essential facilities. The damage can lead to general frustration and mistrust in authorities.

Source: compiled by the authors.

Overall, cyberattacks can have a wide range of consequences for society and the economy. Therefore, it is essential to maintain a high level of cybersecurity to prevent and respond effectively to such attacks.

Cyberattacks and information warfare are often interrelated and can be an essential component of major conflicts and hybrid military operations:

1. Information warfare as a component of hybrid warfare. During hybrid military conflicts, such as Russia's war against Ukraine or the conflict in Syria, information warfare may include the spread of disinformation and propaganda, as well as cyberattacks. Attackers may try to hack into information systems, shut down critical infrastructure, or even spread viruses that affect the operation of systems.

2. Using cyberattacks to support an information campaign. Hackers can use cyberattacks to support their information operations. For example, they can hack into essential facilities or critical infrastructure and use it to prove their version of events or to blackmail adversaries.

3. Response to cyberattacks as part of information warfare. In response to cyberattacks, states and organizations may launch information operations to present evidence or make accusations against the adversary, such as disseminating information about the cyberattack disclosing methods and perpetrators.

4. Using information warfare to launch cyberattacks. Attackers can use information warfare to prepare for cyberattacks. For example, they may collect confidential information or conduct social engineering to gain access to a system (Danyk et al., 2017; Sumets et al., 2022).

Creating an effective cybersecurity strategy is a vital component of protecting against cyberattacks in the modern world. This strategy affects the security of confidential information, as well as the functioning of critical infrastructures, the protection of the rights and interests of citizens, the stability of economic systems, and the country's national security. Such a strategy envisages a comprehensive protection approach (see Figure 4) and includes as follows:

- Analyzing potential threats.
- Developing incident response plans.

- Implementing modern cyber defense technologies.
- Cooperating with parties and conducting regular security audits.

Figure 4 A comprehensive approach to creating an effective cybersecurity strategy.
Source: compiled by the authors.

Only this comprehensive strategy can ensure a high level of cybersecurity and prevent severe consequences of cyberattacks.

The first step is to analyze potential threats and identify weaknesses in one's own systems and infrastructure. It helps to identify what types of cyberattacks could pose the greatest threats. Based on the analysis, the organization creates a cybersecurity strategy that defines the main goals, priorities, and measures to protect information and infrastructure. The strategy should include measures to protect confidential information and user data effectively. This may include encryption, identification and authentication schemes, regular security audits, etc. It is essential to collaborate with other organizations, including industry associations and government agencies, to share information about threats and best practices in cybersecurity. The organization should develop a cyber incident response plan as part of the strategy. It defines how to act in case of an attack and what measures should be taken to restore security (Kovalko et al., 2022).

Protecting personal and corporate information is a vital task in the modern world, where cybercriminals are constantly looking for opportunities to hack into systems and obtain confidential data. Ensuring reliable cybersecurity can prevent severe consequences of incidents and maintain the confidentiality of information. Below, we consider some basic measures and strategies to protect personal and corporate information:

- Strong passwords. It means using complex and unique passwords for accounts and password managers to store passwords and create strong combinations.
- Two-factor authentication. This method requires entering an additional code or using biometric data in addition to the usual password.
- Data encryption. The use of encryption to protect sensitive information on devices and during transmission over the network.
- Antivirus software. This includes the installation of reliable antivirus software to detect and block threats such as viruses and Trojans.
- Software updates. Software updates may include patches against identified weaknesses.
- Protecting against phishing. It means being alert to suspicious emails and websites.
- Network segmentation. The division of the corporate network into segments to limit the possibility of spreading attacks internally.
- Continuous education and training. That means teaching staff about cybersecurity rules and regular training on information security (Furnell & Shah, 2020).

Government institutions play an essential role in ensuring the nation's cybersecurity. Their tasks include regulation and standardization, critical infrastructure protection, cyber leadership, incident response and cyber intelligence, and cyber defense operations. The role of government organizations in ensuring cybersecurity is to create legal, technical, and organizational means to protect the country's information space and ensure the safety of citizens and businesses. Effective protection against cyber threats requires cooperation between government agencies, the private sector, and international partners.

The cyberattack on Ukraine's energy infrastructure (2015-2016) illustrates the role of government organizations in ensuring cybersecurity. Between 2015 and 2016, Ukraine fell victim to a series of cyberattacks on its energy infrastructure. The

attacks resulted in power outages in some regions of the country and caused severe losses to energy companies. This series of cyberattacks was carried out by highly skilled attackers and had a significant impact on Ukraine's energy system. Ukrainian government agencies responded to the attacks and attempted to restore the damaged energy infrastructure. Government agencies conducted investigations to determine who was responsible and the nature of the attacks. As a result of these events, attention to the protection of critical energy infrastructure was increased, and additional security measures were implemented. Ukrainian authorities cooperated with international partners and organizations to identify the source and nature of the cyberattacks and exchange information (Salam et al., 2021).

In 2010, a cyberattack known as Stuxnet occurred in Iran. This attack targeted Iran's nuclear program and affected equipment used for uranium enrichment. The attack caused significant damage and delays to Iran's nuclear project.

In this case, state-sponsored organizations were likely behind the cyberattack. Special services, such as American and Israeli agencies, developed the Stuxnet virus intending to harm Iran's nuclear program. This attack contained new and highly sophisticated cyber weapons and was an essential strategic step in the context of international relations and nuclear security.

This example shows how state organizations can use cyber tools to protect national interests and achieve political goals. Such attacks also emphasize the importance of protecting critical infrastructure and the need for cooperation between countries to ensure cybersecurity.

The cybersecurity sphere constantly evolves as cyber threats become more sophisticated and complex. The main trends in developing cybersecurity are presented in Table 4.

Table 4 Main trends in cybersecurity development.

Trend	Description
Change of authentication methods	New authentication methods, such as biometrics and two-factor authentication, are being used to ensure better cybersecurity.
Geopolitical aspects of cybersecurity	Cybersecurity is becoming an essential element of geopolitical relations, where countries compete for influence and advantages in the digital space.
Changes in approaches to threat detection	Companies are looking for more effective ways to detect and respond to threats using data analytics and machine learning.
Changes in approaches to cybersecurity	Companies are shifting from a traditional approach to cybersecurity to more advanced methods, such as Zero Trust, which involves continuous authentication and traffic monitoring.

Source: compiled by the authors.

These trends indicate the need for continuous development and improvement of cybersecurity measures to protect against cyber threats in the future effectively. Today, special attention is given to Artificial Intelligence (AI) and Machine Learning (ML), which play a crucial role in cybersecurity and are becoming increasingly important in detecting, preventing, and responding to cyber threats. These technologies help enhance security levels in the digital space and address modern challenges in this field.

One of the primary areas of AI and ML applications is threat detection by smart systems. They analyze large volumes of data and identify unusual or suspicious activities in networks, automatically recognizing deviations from normal network connections and alerting about potential threats.

AI and ML also assist in forecasting the nature of threats based on historical data analysis of cyberattacks, which helps improve preparedness for potential risks. They scan software and infrastructure for possible vulnerabilities and analyze user activity to detect suspicious actions.

In the event of a cyberattack, AI can automatically implement measures to restrict the spread of the threat and restore the system to a secure state. They also provide incident response automation and assist in analyzing and identifying vulnerabilities.

Biometric data and other AI aspects are used for enhanced user identification and prevention of unauthorized access. Some countries also employ AI for cyber reconnaissance and cyber defense operations. Applying AI and ML in cybersecurity is crucial for protecting against modern cyber threats and enhancing the effectiveness of cybersecurity measures.

In 2020, the American cybersecurity company FireEye fell victim to a cyberattack during which hackers stole the company's essential security tools. In this case, which became one of the largest cyberattacks in history, FireEye used AI and ML to analyze network traffic and user activity. Thanks to algorithms and artificial intelligence, the system detected anomalies in activity and data movements, indicating unauthorized access.

This example demonstrates how the use of AI and ML in cybersecurity allows for real-time threat detection, analysis of large data volumes, and response to cyberattacks, even in complex scenarios. Artificial intelligence helped FireEye detect security breaches promptly and take measures to limit the damage that could result from this cyberattack.

In our view, cybersecurity is a crucial and constantly evolving shield that safeguards our valuable information, complex systems, and extensive networks from the numerous threats that loom in the digital sphere. As the information landscape

undergoes continuous transformation, the dance between cyber attackers and defenders unfolds with ever-evolving techniques and strategies. The essence of this realm lies in unwavering vigilance, a necessity born from the perpetual metamorphosis of cyber threats. Remaining well-versed in the latest threats, vulnerabilities, and technological advancements becomes the linchpin for adapting defenses with the requisite agility. The foundation of cybersecurity is the management and comprehension of risks. It is crucial to identify potential threats, assess their impact and implement measures to mitigate or manage these risks (Kryshtanovych et al., 2022). To achieve a resilient security posture, a multi-layered defence strategy is essential, involving firewalls, antivirus software, intrusion detection systems, encryption and various security measures combining to create an impervious shield.

In the context of cyber incidents that are centred on humans, the prospect of human error is a significant concern. As a result, a solution can be found in the form of educating employees through comprehensive training on the best practices for cybersecurity. This approach will cultivate an increased awareness of potential threats, including phishing attacks, thereby acting as an effective deterrent. Keeping the digital arsenal up to date is equally imperative. Continuously applying patches and updating software acts as a barrier against exploits targeting known vulnerabilities. Proper orchestration of a well-defined incident response plan is essential in the event of a security breach (Nikonenko et al., 2022). Swift identification, containment, damage mitigation, and restoration of normal operations are the key elements in managing the aftermath of a security incident. Regular security audits and assessments play a central role in proactive measures to strengthen systems and networks against potential vulnerabilities. For example, the Zero Trust security model appears as a sentinel, acknowledging the combined threat of internal and external sources. It emphasizes the importance of verifying identity and offering access only to essential resources, thereby reducing the fertile ground for potential attackers. Artificial intelligence and machine learning technologies step into the fray, enhancing cybersecurity capabilities through the analysis of vast datasets, the identification of patterns, and the early detection of potential threats (Melnyk et al., 2022). Cyber threats, devoid of geographical constraints, demand a global response. International collaboration is not merely a strategy but a prerequisite; it facilitates the exchange of threat intelligence, the sharing of best practices and the coordinated response to cyber incidents globally. In the constantly changing landscape of cybersecurity, the need of the hour is to adopt a proactive and adaptive approach. Organisations and individuals must remain resolute in their dedication to implementing and refining security measures. Only through such steadfastness can we protect sensitive information and maintain the integrity of our digital realms.

5. Conclusions

Cybersecurity today is an integral component of the modern world, where virtually all aspects of our lives have become digital. It impacts the economy, communications, healthcare, and many other spheres. In this context, information warfare and cybersecurity are closely interconnected. Information operations and cyberattacks have become tools for achieving political, economic, and military objectives.

With the use of artificial intelligence and machine learning technologies, cybersecurity gains new capabilities. These technologies help detect threats, analyze vast amounts of data, and respond to cyberattacks in real time.

In the fight against cyber threats, international cooperation becomes exceptionally important. Since cyber threats have no borders, countries must collaborate to develop cybersecurity standards and share threat intelligence for effective countermeasures.

In the future, cybersecurity will remain one of the most crucial issues and one of the most complex and dynamic fields. The development of new technologies, such as quantum computing, quantum cryptography, advanced artificial intelligence, and machine learning, as well as the development of the Internet of Things (IoT), create new challenges and opportunities in the field of cybersecurity.

Ethical considerations

Not applicable.

Conflict of Interest

The authors declare no conflicts of interest.

Funding

This research did not receive any financial support.

References

Aghajani, G., & Ghadimi, N. (2018). Multi-objective energy management in a micro-grid. *Energy Reports*, 4, 218-225.

Akhavan-Hejazi, H., & Mohsenian-Rad, H. (2018). Power systems big data analytics: An assessment of paradigm shift barriers and prospects. *Energy Reports*, 4, 91-100.

Al-Ghamdi, M. I. (2021). *Effects of knowledge of cyber security on prevention of attacks*. Materials Today: Proceedings.

Alkatheiri, M. S., Chaudhary, S. H., & Alqarni, M. A. (2021). Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. *Sustainable Energy & Technology Assessment*, 45.

Amir, M., & Givargis, T. (2020). Pareto optimal design space exploration of cyber-physical systems. *Internet of Things*.

Borodina, O., Kryshtal, H., Hakova, M., Neboha, T., Olczak, P., & Koval, V. (2022). A conceptual analytical model for the decentralized energy-efficiency management of the national economy. *Polityka Energetyczna*, 25(1), 5-22. https://doi.org/10.33223/epj/147017

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2021). Cybersecurity and critical infrastructure protection. In *Introduction to Homeland Security* (6th ed., Chapter 8, pp. 425-497). Butterworth-Heinemann.

Bystrova, B. (2019). Levels of quality assurance of cybersecurity specialists training in US higher education institutions. *Pedagogical sciences: theory, history, innovative technologies*, 2(86), 140-149.

Cao, Y., et al. (2019). A topology-aware access control model for collaborative cyber–physical spaces: Specification and verification. *Computers & Security*, 87.

Danyk, Yu. H., Vdovenko, S. H. (2017). Conceptual directions of a comprehensive solution to an information security problem in the system of the armed forces covert control. *Modern Information Technologies in the Sphere of Security and Defence*, 2(29), 98-107.

Dash, N., Chakravarty, S., & Satpathy, S. (2021). *An improved harmony search-based extreme learning machine for intrusion detection system*. Materials Today: Proceedings.

Furnell, S., & Shah, J. N. (2020). Home working and cyber security – an outbreak of unpreparedness? *Computer Fraud & Security*, 2020(8), 6-12.

Ji, Z., et al. (2021). Harmonizing safety and security risk analysis and prevention in cyber–physical systems. Process Safety and Environmental Protection, 148.

Karbasi, A., & Farhadi, A. (2021). A cyber-physical system for building automation and control based on a distributed MPC with an efficient method for communication. *European Journal of Control*.

Kovalko, O., Eutukhova, T., & Novoseltsev, O. (2022). Energy-related services as a business: Eco-transformation logic to support the low-carbon transition. Energy Engineering: *Journal of the Association of Energy Engineering*, 119(1), 103-121. https://doi.org/10.32604/EE.2022.017709

Kryshtanovych, M., Akimova, L., Akimov, O., Kubiniy, N., & Marhitich, V. (2021). Modeling the process of forming the safety potential of engineering enterprises. *International Journal of Safety and Security Engineering*, 11(3), 223-230. https://doi.org/10.18280/ijsse.110302

Kuzmenko, B.V., Zaika, Yu.O. (2012). Cyberterrorism: Global and Ukrainian Realities. *Scientific Journal of the National Academy of Internal Affairs*, 2(81), 92-98.

Levytska, S., Pershko, L., Akimova, L., Akimov, O., Havrilenko, K., & Kucherovskii, O. (2022). A risk-oriented approach in the system of internal auditing of the subjects of financial monitoring. *International Journal of Applied Economics, Finance and Accounting*, 14(2), 194-206. https://doi.org/10.33094/ijaefa.v14i2.715

Melnyk, D. S., Parfylo, O. A., Butenko, O. V., Tykhonova, O. V., & Zarosylo, V. O. (2022). Practice of the member states of the european union in the field of anti-corruption regulation. *Journal of Financial Crime*, 29(3), 853-863. https://doi.org/10.1108/JFC-03-2021-0050

Motsch, W., et al. (2020). Approach for dynamic price-based demand side management in cyber-physical production systems. *Procedia Manufacturing*, 51.

Nguyen, D. C. L., & Golman, D. W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs. 'law in action.' *Computer Law & Security Review*, 40.

Nikonenko, U., Shtets, T., Kalinin, A., Dorosh, I., & Sokolik, L. (2022). Assessing the policy of attracting investments in the main sectors of the economy in the context of introducing aspects of industry 4.0. *International Journal of Sustainable Development and Planning*, 17(2), 497-505. https://doi.org/10.18280/ijsdp.170214

Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. *Computers & Security*, 108.

Qiu, W., et al. (2021). Time-frequency-based cyber security defense of wide-area control system for fast frequency reserve. *International Journal of Electrical Power & Energy Systems*, 132.

Salam, S., et al. (2021). A survey of cyber security management in industrial control systems. *Computers & Security*, 102.

Srinivasan, S., & Srivastava, S. (2021). Cyber-security risk management: Indian automobile sector. *Computers & Security*, 106.

Sumets, A., Kniaz, S., Heorhiadi, N., Skrynkovskyy, R., & Matsuk, V. (2022). Methodological toolkit for assessing the level of stability of agricultural enterprises. *Agricultural and Resource Economics*, 8(1), 235-255. https://doi.org/10.51599/are.2022.08.01.12

Tavolato, P. P., et al. (2021). Network protocol independent anomaly detection using deep learning autoencoders. *Future Generation Computer Systems*, 80-96.

Uwitonze, P., et al. (2021). Hybridized elliptic curve cryptography-based group signature scheme for secure IoT-enabled telemedicine systems. *Journal of Medical Systems*, 45(6), 1-14.

Wang, J., et al. (2021). A survey of threat intelligence in IoT security. *Future Generation Computer Systems*, 116.

Wang, X., et al. (2021). Communication-efficient secure data aggregation for distributed cyber-physical systems. *Future Generation Computer Systems*, 118.

Yang, M., et al. (2021). *A hybrid quantum-behaved particle swarm optimization with differential evolution and fuzzy clustering algorithm for clustering analysis*. Materials Today: Proceedings.

Zhang, Y., et al. (2021). Dynamic cyber risk assessment for industrial control systems: A data-driven approach. *Reliability Engineering & System Safety*, 210, 107568.

Zulkurnain, N. S., et al. (2021). IoT-based electronic health record access control and management. Journal of King Saud University - Computer and Information Sciences.