Journal of Political Science: Bulletin of Yerevan University
2025, VOL. 4, NO. 1 (10), 110-124
https://doi.org/10.46991/JOPS/2025.4.10.110

JOPS

NEW CYBERSECURITY CHALLENGES: DIGITAL TRANSFORMATION AND THE POLITICAL IMPLICATIONS OF THEIR IMPLEMENTATION

ANNA SISOYAN *
Yerevan State University

Abstract

The purpose of this article is to analyze modern challenges in the field of cybersecurity and mechanisms for countering cyber threats, assess the problems our country faces in this area, and identify possible solutions. To achieve this goal, the article studies the basic concepts related to cyberspace, considers real examples of cyber attacks recorded in recent years, and studies the experience, legislative and institutional framework of the leading countries in this area. In this context, the author highlights the structural similarities and differences of the countries in question. The relevance of this article is due to the analysis of new challenges to cybersecurity and the growing scale of application of information technologies in all spheres of human political activity. In the era of digitalization, information is acquiring the status of the most important object, a strategic resource of both the state and any management structure in the political management system. In this context, the relevance of the research topic is manifested in the development of the concept of a knowledge and information society developing on the basis of modern information and communication technologies. Information as a strategic resource requires a special state attitude not only in terms of its development and accumulation, but also protection. The article also analyzes the development of new information technologies, which causes an increase in the technological gap between the increasingly complex requirements for information resource security indicators in all countries and the capabilities of information technologies and software and hardware used to ensure information security.

Keywords: *cybersecurity, cyberspace, cyberwar, cyberattack, cyberterrorism, cyber diplomacy, cyber activism, hacking.*

Introduction

The development of modern technologies has not only enabled the implementation of various informational activities but has also made the information field physically vulnerable. Access to the internet, the creation of user accounts, and the use of modern

* **Anna Sisoyan** is a PhD candidate of the Chair of Political Science of the Faculty of International Relations at Yerevan State University. Email: anna.sisoyan@ysu.am. ORCID: https://orcid.org/0009-0009-6170-5366.

Received: 22.04.2025
Revised: 15.05.2025
Accepted: 20.05.2025

online communication tools have become imperatives of the times. Alongside these advancements, significant attention is being paid to security measures. Programs and antivirus software are being developed to protect systems from attacks. However, hacking technologies are also rapidly evolving, often outpacing security systems. As a rule, antiviruses and other protective measures are reactive, responding to already-occurred attacks or newly created viruses. In this regard, cybersecurity and the protection of cyberspace have become critically important.

Cyber threats pertain to the security of individuals, organizations, and states. It is the responsibility of each state to protect the security of its citizens, organizations, and critical infrastructure. States develop policies to ensure the security of cyberspace. Many countries have strategies that define the guidelines states must follow in order to remain as secure as possible in cyberspace and, more broadly, in the information domain. In the modern world, wars are fought not only through armed conflicts but also via informational and cyber attacks. Often, the battle takes place solely in the cyber or information domain, which is why being "armed" in cyberspace has become an imperative of our time. It is worth noting that there is a growing need for scientifically based methods and technological solutions to update and improve the information security system, but the difficult process of scientific and practical developments in the field of creating information security tools and software and hardware systems cannot provide a solution to this problem. As the cyber domain evolves rapidly, the threats associated with it demand not only offensive actions but also defensive strategies. Cyber attacks can impact the security of states, their economic prosperity, and public stability by disrupting critical infrastructure, stealing sensitive information, damaging or disabling services, and causing panic. Therefore, states must include not only military or law enforcement forces in their defense strategies but also specialized teams focused on cybersecurity and information protection.

This is a complex process that requires international cooperation, rapid response mechanisms, education, and the development of knowledge in the field of cybersecurity. States need to collaborate with international organizations, the private sector, and public organizations, pooling resources and expertise to mobilize their defenses in cyber conflict.

Mechanisms for preparedness in cyberspace imply not only the creation of technical measures, but also the adoption of strategic decisions to respond to future threats. In this context, it is useful to study the experience of leading countries of the world, since Armenia is also making efforts to create institutional mechanisms for regulating the sphere and counteracting existing and potential threats in cyberspace.

What is cyberspace?

There are various definitions and descriptions of cyberspace, and the term began to be used as early as the 1980s. Interestingly, its first use was found in William Gibson's (1984) science fiction novel Neuromancer. It is clear that the artistic depiction of cyberspace, especially in a science fiction book, significantly differs from its contemporary meaning (Singer and Friedman 2014; Murphy 2024).

Over time, attempts have been made to define the concept. The efforts have involved the U.S. Department of Defense and the Pentagon. In 2008, the Pentagon assembled a team of experts, which took nearly a year to define cyberspace. It was defined as a "global domain within the information environment, consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and control systems." (US Air Force 2023).

According to another definition, cyberspace is a virtual computer world, specifically the electronic means used to facilitate interaction and communication through a globally interconnected network of systems. It encompasses a vast network of computers consisting of numerous global subnetworks that use the TCP/IP (Transmission Control Protocol and Internet Protocol) protocols for communication and data exchange (Raghad et al. 2024).

Cyberspace enables users to exchange information, conduct business, and create interactive media, among numerous other activities. In the modern cyberspace, artificial intelligence plays a crucial role in shaping virtual interactions—from personalized news feeds to AI-powered chatbots that increase user experiences (Li and Bai 2025). In other words, cyberspace is the virtual, networked domain where any network-based activity is possible, and anyone with access to the global network can be its user. Cybersecurity, in turn, is the security of cyberspace. Just as physical state territory is an object of international relations, the question of the objectivity of cyberspace also arises. Gradually, cyberspace is becoming a subject of interdisciplinary discussion and is aspiring to become an object of international relations as well as international law. In this regard, discussions about establishing regulations related to cyberspace are intensifying across various levels.

Numerous economic, social, and political regulations related to cyberspace have been implemented at local, national, and international levels. Notably, security has taken central stage as a critical factor influencing intergovernmental cooperation. Information and communication technologies have significantly impacted international relations, reshaping interactions between international organizations, their members, and other stakeholders of the information society. These technologies have fostered the development of horizontal networks, which complement rather than replace existing hierarchical structures.

Currently, the international institutional framework for cyberspace governance is witnessing a surge in initiatives aimed at enhancing cooperation at the global level. This includes a redistribution of roles among existing actors. Such dynamics can be seen as a cornerstone for ensuring security within cyberspace and expanding the information society. To date, states have largely promoted existing global institutions by assuming responsibilities related to the cyber domain and reshaping their agendas to address these emerging challenges.

Efforts to adapt theories of international relations to the demands of the information society remain limited, primarily because the focus has largely been on the development of internal (domestic) regulations. Attempts to create conceptual frameworks rarely build on one another, making it difficult to advance comprehensive

concepts or intermediary theories grounded in interdisciplinary approaches (Kremer and Müller 2014).

Dimensions of cybersecurity assurance

Cybersecurity encompasses any technology, activity, or policy aimed at preventing cyberattacks or mitigating their impact (Singh 2025). Its primary goal is to safeguard computer networks, applications, devices, data, financial assets, and individuals from malicious software, fraud, data theft, deception, and other cyber threats (Tabrizchi and Aghasi 2025).

Cybersecurity is critical because cyberattacks and cybercrimes have the potential to disrupt, harm, or destroy businesses, communities, and lives. Successful cyberattacks can result in identity theft, personal and corporate extortion, disruption of business operations, loss of sensitive information and critical business data, which in turn may lead to the loss of customers and even the closure of businesses (Beuran 2025; Jøsang 2025).

The importance of cybersecurity extends beyond personal and business domains. Its significance is increasingly evident in international relations, driven by the growing reliance of states on digital infrastructure and the internet. Cyberattacks have become threats to national security, targeting economic, political, and military sectors. Infrastructure-focused cyberattacks can be carried out by both independent hacking groups and state actors. Some states are even creating cyber armies not only to counter potential cyber threats but also to conduct their own offensive cyber operations. These attacks can serve various purposes and objectives, making no state immune to cyber threats. Consequently, in recent years, states have intensified their cooperation in the cyber realm to achieve greater security. In this context, the concept of ‘cyber diplomacy’ has emerged, referring to a set of tools and strategies employed by states, groups, and individuals to conduct their activities in cyberspace (Paulus 2024). The goal of cyber diplomacy is to protect national interests and foster relationships in political, economic, cultural, and scientific domains during peacetime (Chihaia and Rempala 2023).

Cyber diplomacy encompasses the use of diplomatic tools and initiatives to achieve objectives in the complex and continuously evolving cyberspace. States rely on universally accepted rules, protocols, and customary laws, both codified and informal, to facilitate collaboration among global public and private sector stakeholders.

Cyber diplomacy is expected to mitigate the consequences of cyber aggression against critical infrastructure, cyberattacks, data breaches, cybercrimes, cyber espionage, online theft, and other disruptive cyber operations carried out by both state and non-state actors. Given the nature of cyberspace, proactive cyber diplomacy is deemed more effective than relying solely on reactive cyber defense measures.

State and non-state actors actively use cyberspace and the internet for manipulation, service disruption, fraud, extortion, data theft, and money laundering. The internet has become a stage for geopolitical conflicts and the dissemination of disinformation. In this context, the political dimension is particularly significant. Cyberattacks are also employed during election campaigns, such as the U.S. presidential elections,

Emmanuel Macron's campaign, the German Bundestag elections, and others (Williams and Rowe 2025).

Notable examples of cyber attacks

Among the major recorded cyberattacks is the series of attacks on the American company SolarWinds. Between 2019 and 2020, a group of hackers (known as Nobelium by Microsoft or SolarWinds Hackers) targeted the Orion system, gaining access to the networks, systems, and databases of SolarWinds' clients. As a result of the attack, the hackers were able to access not only the data and computers of Orion users but also the data of SolarWinds' partners and clients using other software. Companies such as Microsoft, Intel, Cisco, and Deloitte were among those affected by this cyberattack (Amador et al. 2025). Following this series of attacks, many stakeholder organizations strengthened their security systems by implementing mechanisms to prevent and quickly neutralize future cyberattacks (Oladimeji and Kerner 2023).

As noted, due to geopolitical circumstances, cyberattacks often target specific states and their infrastructures. An example of such an attack is the NotPetya cyberattack, which primarily targeted Ukraine. The attack began in June 2017, and from the outset, Russia was accused of being behind it. Notably, at the time, Russia and Ukraine were not engaged in active warfare, meaning the attack occurred during a period of relative peace.

The consequences of the attack were severe, affecting a large number of individuals and organizations. The attack was carried out using a modified hacking program that completely erased users' data from computers. In some cases, victims were asked to pay ransoms in bitcoin to recover their data (Möller 2023). However, even after making payments, no data was restored, and it was practically impossible to recover the deleted information.

It should also be noted that the attack did not only harm Ukraine and Ukrainian organizations but also caused significant damage to other countries and their entities. The effects of this cyberattack were felt in the United States, Poland, Germany, France, and several other nations (Stoddart 2022).

During the ongoing Russia-Ukraine war, hostilities have extended into the cyber realm. Since the conflict began, both sides have attempted to disrupt each other's infrastructures, damage networks and control systems, and acquire intelligence data (Brantly and Brantly 2024). In quantitative terms, Russian cyber operations have become more intense, as the majority of cyber attacks carried out by the Russian side since 2014 and more intensively since 2022 are destructive in nature (Bronk, Collins and Wallach 2023).

Ukraine's efforts in the cyber domain are primarily focused on neutralizing threats originating from Russia. Offensive operations, on the other hand, are aimed at disrupting critical infrastructure. Specifically, there have been attempts to destabilize the functioning of banking systems, certain administrative websites, and airport operations (Tavakkoli et al. 2025).

The Arab-Israeli conflict also features numerous elements of cyber warfare. On October 7, 2023, Hamas' attack on Gaza was accompanied by cyberattacks primarily

targeting critical infrastructure, telecommunications systems, energy supplies, and transportation networks (Mizobuchi 2025). These actions were labelled as cyberterrorism by Israel. It is worth noting that these cyberattacks had a significant impact on Israeli society, causing both material and psychological harm (Singh and Bajeje 2025).

Israel's cyber operations are not as overt as those of its adversaries; however, the country does engage in cyber activities, primarily utilizing espionage software. In recent years, there has been significant discussion about the Israeli-made Pegasus software, developed by the NSO Group (Kotliar and Carmi 2023). According to its creators, Pegasus is designed to assist in uncovering money laundering, drug trafficking, and terrorism (Kaster and Ensign 2022).

In recent years, cyberactivism has also been gaining momentum. Perhaps the most prominent group in this sphere is Anonymous, which began its activities in the early 2000s and continues to operate today. The group is known for organizing protest actions, conducting cyberattacks, and orchestrating information leaks. This type of activist (known as hacktivists) advocates for information freedom and opposes censorship. Anonymous was one of the groups that supported WikiLeaks, which had disclosed a series of classified documents to the public (Romano 2024).

In recent times, the number of cyberattacks attributed to China has significantly increased. This June, several countries, including Australia, Germany, the United States, the United Kingdom, Canada, New Zealand, South Korea, and Japan, detected cyber activities conducted by China within their networks. This was not the only instance this year when various governments reported cyber operations targeting their networks, allegedly carried out by China (Wade 2023; Singh and Bajeje 2025).

Institutional mechanisms of cybersecurity

Many countries have a cybersecurity strategy that defines and guides the measures to be implemented to neutralize potential threats to cyberspace. Among these countries is the Federal Republic of Germany, which has developed a comprehensive cybersecurity doctrine[1]. In a modern high-tech and digitized industrial nation like Germany, the security and functionality of the state, economy, and society are heavily reliant on digital processes and infrastructures (Couretas 2022).

Germany, too, has seen a year-by-year increase in the number of cyberattacks, carried out by both state and non-state actors. One of the Federal Government's primary responsibilities is ensuring the safety of the country, its society, and its citizens. Citizens rightfully expect their government to protect the state and society from digital threats.

In the Federal Republic of Germany, responsibility for cyber security lies with the Federal Ministry of the Interior and Community, which has developed a Cyber Security Concept[2]. As part of its cyber security strategy, the Federal Government has

[1] Bundesministerium der Verteidigung. 2021. "Cyber-Sicherheitsstrategie." Accessed January 21, 2025. https://www.bmvg.de/de/themen/cybersicherheit/partnerschaften-zur-cybersicherheit/cyber-sicherheitsstrategie--12078.

[2] Federal Ministry of the Interior. 2025. "Cyber Security and Digital Policy." Accessed January 21, 2025. https://www.bmi.bund.de/EN/topics/it-internet-policy/it-internet-policy-node.html.

established measures to protect information and communication technologies, with a focus on cooperation between government agencies and the involvement of relevant societal groups.

Particularly important bodies in this context are the National Coordination Centre for Cybersecurity (NCC-DE)[3], which implements the main goals and objectives of the Cybersecurity Strategy. Nevertheless, the internet never stops. Cybersecurity is an issue that requires constant, round-the-clock vigilance and the integration of cutting-edge technologies for its maintenance. The Federal Armed Forces (Bundeswehr) aim to strategically harness the potential of innovations and actively participate in the so-called 'digital startup ecosystem' (Kayser, Telukdarie and Philbin 2023). This is precisely why the Cyber Innovation Hub was established, serving as a bridge between startups and the Bundeswehr.

The Federal Armed Forces (Bundeswehr) actively cooperate with NATO's Cooperative Cyber Defence Centre of Excellence. Every year, ICT experts from the ministry and the Bundeswehr take part in the Locked Shields exercise. During this exercise, a simulated cyber attack scenario is created and the participants must work to neutralise the attack.

France, like other EU countries, is making significant efforts to ensure cybersecurity. The French National Cybersecurity Strategy was updated in 2021. It is part of the national defense and security doctrine, focusing on the protection of critical national infrastructures, the growth of digital diplomacy, and the development of offensive cyber capabilities.

The National Agency for the Security of Information Systems (ANSSI) plays a key role in the new cyber environment around France and the EU, investing in and working on nine strategic areas that must be implemented by 2030[4]. All of this demonstrates France's determination to take a leading role in ensuring cybersecurity within the EU (Vitel and Bilddal 2015; Vogiatzoglou 2025).

The UK is one of the leading countries in cybersecurity within the European region. The UK's Cybersecurity Strategic Document is updated regularly, with the latest update in 2022. The UK's Cyber Security Strategy document is regularly updated, most recently in 2022, which looks at the challenges in this area, the UK's vision and the five key pillars of cyber security[5]. The Strategy highlights the UK's commitment to a balance between the public, private and third sectors in addressing cyber security challenges. In addition to the National Cyber Strategy, the United Kingdom has

[3] Federal Office for Information Security. 2025. "National Coordination Centre for Cybersecurity (NCC-DE)." Accessed January 21, 2025. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/NKCS/nkcs_node.html.

[4] Ministry for Europe and Foreign Affairs. 2025. "France and Cyber security." Accessed January 21, 2025. https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/; ANSSI. 2023. "The French approach to cyber." *November 28, 2023*. Accessed January 21, 2025. https://cyber.gouv.fr/en/french-approach-cyber-0.

[5] Cabinet Office. 2022. "Policy paper: National Cyber Strategy 2022." *December 15, 2022*. Accessed January 21, 2025. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

another strategic document related to the field: the Government Cyber Security Strategy for 2022-2030[6].

The primary body responsible for cyber security in the UK is the National Cyber Security Centre (NCSC), as its activities focus on protecting critical infrastructure, responding to incidents, developing cyber security guidance, providing advice and ensuring international cooperation. Although the government also plays a role in implementing measures to strengthen cyber security, as outlined in the government's key cyber security strategy documents, the primary responsibility lies with the NCSC (Montasari 2023; Lamb 2025).

The first document is broader in scope, emphasizing the security of various infrastructures and addressing both domestic and international efforts to strengthen cybersecurity and the UK's role in these endeavours. In contrast, the 2022-2030 Strategy focuses specifically on the government's actions to bolster cybersecurity and achieve the set objectives.

The Russian Federation is also taking active steps to increase its capabilities in this area, and Cybersecurity is considered in the Doctrine of Information Security of the RF in 2016. It is noteworthy that this Doctrine does not use the term "cybersecurity", but uses the term "information security" instead. At the same time, Russia's information security is considered a matter of national interests, and threats to information security are considered threats to national security (Bartnicki, Kużelewska and Ożóg 2023).

The importance of ensuring Russia's information security is emphasized, along with defining the bodies responsible for it and the resources and measures that play a critical role in securing the Federation's information security (Konovalova, Kandrina and Kazantseva 2023). This Doctrine is entirely devoted to protection against information threats, especially emphasizing threats coming from foreign countries that may have military objectives. It also emphasizes the potential danger coming from terrorist and extremist groups. In addition, it emphasizes the negative impact of computer crimes on the financial and economic sectors, and also defines strategic goals and directions for achieving information security.

In the Russian Federation, cybersecurity is also prioritized at the institutional level. Several agencies are responsible for cybersecurity and information security, with the most significant being: 1) The Federal Security Service (FSB); 2) The Ministry of Digital Development, Communications, and Mass Media; 3) The Federal Service for Technical and Export Control; 4) The National Coordination Center for Computer Incidents; 5) The Ministry of Defense.

In the knowledge and digital society, the United States of America is undoubtedly the leading country in this area. The key document in this domain is the National Cybersecurity Strategy[7]. Alongside this strategy, there are numerous other legislative documents and a range of agencies whose core mission is to ensure cybersecurity. These include: 1) The Department of Homeland Security (DHS); 2) The National

[6] Cabinet Office. 2022. "Policy paper: Government Cyber Security Strategy: 2022 to 2030." *February 17, 2022*. Accessed January 21, 2025. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

[7] The White House. 2023. "The National Cybersecurity Strategy." Accessed January 21, 2025. https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/.

Security Agency (NSA); 3) The Cybersecurity and Infrastructure Security Agency (CISA).

Notably, the U.S. adopted its first cybersecurity strategy document back in 2003, which was periodically updated and renamed over time until 2023. The latest version of the National Cybersecurity Strategy, like the UK, identifies a number of key pillars:

- Protect critical infrastructure,
- Disrupt and dismantle threat actors,
- Build capabilities to ensure security and resilience,
- Invest in a more resilient future,
- Forge international partnerships based on shared goals.

These pillars reflect the U.S.' comprehensive approach to national and global cybersecurity as it emphasizes its leadership role in this area and not only strives to maintain domestic security but also seeks to act as a unifier and leader on the international stage. As seen, the abovementioned countries possess both institutional and doctrinal preparedness to counter cyber threats. In the cases of France and the UK, responsibility for the field lies with specialized institutions—namely, the National Agency for the Security of Information Systems (ANSSI) and the National Cyber Security Centre (NCSC). In contrast, for Germany and Russia, the primary coordinators are ministries, notably with the involvement of their defense ministries. In the U.S., both the government and individual agencies play a significant role.

The strategic documents of all these countries generally highlight the importance of countering external threats, protecting critical infrastructures, incorporating innovative technologies into cybersecurity measures, and fostering international collaboration (Uslu 2024). A commitment to assuming a leadership role in the field is particularly evident in the case of the U.S. (Özdemir and Yıldız 2024).

The five-pillar approach in the UK and US strategies is also noteworthy, as although the titles of their strategies differ, there are clear similarities in the content, particularly in the context of protecting infrastructure, building resilience and taking a visible role in the international arena. In this context, it is also important to note that these strategic documents are periodically updated, which a natural necessity is given the rapid changes in cyberspace and technology, as well as the emergence of new challenges and threats.

Institutional mechanisms of Cybersecurity in the Republic of Armenia

Armenia has implemented and continues to develop mechanisms for regulating cyberspace, where the fight against cyber threats is a priority for the country. Given its participation in a hybrid war, Armenia is not immune to external cyber attacks, which require significant efforts not only to counter and neutralize, but also to detect (Elamiryan and Margaryan 2018).

The National Security Strategy of Armenia (2020) addresses the cyber domain. In the section titled "Ensuring Open and Secure Information and Cyberspaces," it highlights the following challenges: 1) the lack of a comprehensive state policy in the field of information and cybersecurity; 2) the absence of legislation ensuring the protection of critical information infrastructures; 3) insufficient institutional capacities

of computer incident response structures; 4) the absence of a coordinating body for cybersecurity[8].

This strategic direction emphasizes Armenia's commitment to improving its institutional framework and capabilities to address cyber threats effectively (Spînu 2020).

Since 2023, the draft Law on Cybersecurity of the RA has been introduced and is currently under discussion. The draft states that "relations arising in the field of ensuring cybersecurity are regulated by the Constitution, this law, international treaties of the RA, other laws, and legal acts adopted on their basis."[9] It also specifies that "the state policy in the field of cybersecurity is developed and implemented by the body authorized under the Law on the Structure and Activities of the Government."[10]

The draft law further defines:

- The functions of the body responsible for implementing cybersecurity policy,
- Measures to ensure the cybersecurity of critical infrastructures in emergency situations,
- The responsibilities of persons accountable for cybersecurity,
- Plans for establishing a Computer Emergency Response Team,
- Requirements for cybersecurity service providers,
- Mechanisms for monitoring compliance with the law and legal acts adopted based on it[11].

The adoption of the law would be a significant step forward in regulating the field. In the RA, gaps related to cybersecurity are evident at the institutional level as well; there is no primary governing body overseeing the field. Challenges in the cyber domain are currently addressed by the National Security Service, Police, Ministry of Defense, and, in the context of international treaties, the Ministry of Foreign Affairs. The establishment of a coordinating body would enable a more systematic approach to addressing these challenges.

Post-war Armenia's efforts have primarily focused on neutralizing cyberattacks and their consequences, such as Azerbaijan's (Ismailzade 2024) use of the Pegasus spyware to monitor the phones of Armenian citizens. However, preventing such attacks would be a far more effective approach. Organizing and mitigating such attacks require substantial material and human resources. Given its limited resources, the RA must optimize their use and eliminate any potential oversights.

Efforts must be undertaken by both the public and private sectors. The protection of critical infrastructures should be prioritized, as any disruption in their operation due to cyberattacks could lead to irreversible consequences and significant losses. For Armenia, it is crucial to study the experiences of leading countries in the field and implement mechanisms that address the country's unique challenges. This does not

[8] MFA. 2020. "National Security Strategy of the Republic of Armenia: A Resilient Armenia in a Changing World." Accessed January 21, 2025. https://www.mfa.am/filemanager/security%20and%20defense/Armenia%202020%20National%20Security%20Strategy.pdf.

[9] The Draft of Law on Cybersecurity of the RA. Accessed January 21, 2025. https://www.e-draft.am/projects/6656/about.

[10] Ibid.

[11] Ibid.

imply copying the legislation or practices of any specific country but rather adapting the best practices to Armenia's specific circumstances (Aleksanyan 2024; Poghosyan 2022).

Conclusion and discussion

In conclusion, it can be stated that alongside technological advancements, the importance of cyberspace has grown significantly, and countering cyber threats has become one of the primary challenges for states. Countries are developing legislative frameworks and establishing relevant institutions to regulate the cyber domain, as well as engaging in international cooperation to jointly address existing and potential threats. For some countries, particularly those involved in active conflicts, it is crucial not only to counter internal and external cyber threats but also to organize offensive cyber operations.

The Republic of Armenia is not immune to cyber threats and, as a party to an active conflict, must invest more robust efforts in addressing threats in the field. Given the gaps at both the legislative and institutional levels, it is essential to intensify efforts toward their development. In this context, studying the experiences of countries with successful outcomes in the field, implementing necessary mechanisms, and optimizing resources can be highly beneficial for Armenia.

The development of information and communication technologies creates new challenges and threats to the national security of post-war Armenia, since the information space is used by Azerbaijan to achieve military-political, geopolitical and other goals. The increase in the dynamics and scale of economic and information threats in post-war Armenia causes a discrepancy between the required and existing levels of organization of management decision-making processes and information interaction of state, public and private structures in the field of security, which is especially characteristic of Armenia due to insufficient funding, imperfections in interdepartmental scientific and technical policy, and a weak level of development and implementation of information technologies. At the same time, insufficient protection of information resources leads to the leakage of important political, economic, scientific and military information. Along with new opportunities, these technologies have created previously non-existent challenges for government officials. Armenia, included in global interaction processes, is experiencing changes related to the transformation of communication processes. Since our country has post-war consequences. It is worth noting that the existing human resources, material and information resources do not provide an adequate response to the centripetal growth and development of threats emanating from the information space, which increases the scale of damage from their impact on cybersecurity systems.

Acknowledgments
The author would like to thank the anonymous reviewers for their insightful comments and critiques.

Conflict of interests
The author declares no ethical issues or conflicts of interest in this research.

Ethical standards
The author affirms this research did not involve human subjects.

References

Aleksanyan, Ashot. 2024. "Hybrid War against European Political Integration of Armenia: A Dead End or a Springboard on the Way to the EU?." In: *The 'New' Geopolitics in the Caucasus What Role for the EU?*, edited by Gvantsa Davitashvili, Thomas Kruessmann, and Ivanna Machitidze, 123-144. Hannover; Stuttgart: ibidem-Verlag.

Amador, Tristen et al. 2025. "An Interdisciplinary Thematic Analysis of the US National Guard Bureau Response to the SolarWinds Attack." In: *Human Aspects of Information Security and Assurance. HAISA 2024. IFIP Advances in Information and Communication Technology, vol 721*, edited by Nathan Clarke, and Steven Furnell, 264-277. Springer, Cham. https://doi.org/10.1007/978-3-031-72559-3_18.

Bartnicki, Adam R., Elżbieta Kużelewska, and Michał Ożóg. 2023. "Information and Information Technologies in the 2022 Russian-Ukrainian War." In: *War in Ukraine. Media and Emotions*, edited by Agnieszka Turska-Kawa, Agnieszka Kasińska-Metryka, and Karolina Pałka-Suchojad, 21-41. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-37608-5_3.

Bellabarba, Giulia. 2024. "NotPetya: Understanding the Destructiveness of Cyberattacks." *Security Outlines, January, 28 2024*. Accessed January 21, 2025. https://www.securityoutlines.cz/notpetya-understanding-the-destructiveness-of-cyberattacks/.

Beuran, Razvan. 2025. Cybersecurity Awareness Training. In: Cybersecurity Education and Training. Springer, Singapore, pp. 153-170. https://doi.org/10.1007/978-981-96-0555-2_8.

Brantly, Aaron F., and Nataliya D. Brantly. 2024. "The Bitskrieg That Was and Wasn't: The Military and Intelligence Implications of Cyber Operations during Russia's War on Ukraine." *Intelligence and National Security* 39 (3): 475-495. https://doi.org/10.1080/02684527.2024.2321693.

Bronk, Chris, Gabriel Collins, and Dan S. Wallach. 2023. "The Ukrainian Information and Cyber War." *The Cyber Defense Review* 8 (3): 33-50.

Chihaia, Mihai Sebastian, and Jan Rempala. 2023. "Cyber Diplomacy." In: *The Palgrave Encyclopedia of Global Security Studies*, edited by Scott N. Romaniuk, and Péter N. Marton, 260-264. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-74319-6_27.

Couretas, Jerry M. 2022. Cyber Policy, Doctrine, and Tactics, Techniques, and Procedures (TTPs). In: An Introduction to Cyber Analysis and Targeting. Springer, Cham, pp. 13-36. https://doi.org/10.1007/978-3-030-88559-5_2.

Elamiryan, Ruben, and Mamikon Margaryan. 2018. "Cyber Security in the Context of Armenia-NATO Cooperation." *Journal of Information Warfare* 17 (1): 99-111.

Gibson, William. 1984. Neuromancer. Ace.

Ismailzade, Fariz. 2024. "Digital Diplomacy in Azerbaijan: Lessons Learned and Future Opportunities." In: *Digital Diplomacy in the OSCE Region: From Theory to*

Practice, edited by Erman Akıllı, Burak Güneş, and Oğuz Güner, 11-19. Springer, Cham. https://doi.org/10.1007/978-3-031-50966-7_2.

Jøsang, Audun. 2025. Governance and Information Security Management. In: Cybersecurity: Technology and Governance. Springer, Cham, pp. 377-403. https://doi.org/10.1007/978-3-031-68483-8_18.

Kaster, Sean D., and Prescott C. Ensign. 2022. "Privatized espionage: NSO Group Technologies and its Pegasus spyware." *Thunderbird International Business Review* 65 (3): 355-364. https://doi.org/10.1002/tie.22321.

Kayser, Kenneth, Arnesh Telukdarie, and Simon P. Philbin. 2023. "Digital Start-Up Ecosystems: A Systematic Literature Review and Model Development for South Africa." *Sustainability* 15 (16), 12513: 1-24. https://doi.org/10.3390/su151612513.

Konovalova, Lyudmila G., Nadezda A. Kandrina, and Olesia L. Kazantseva. 2023. "Amendments to the Constitution of the Russian Federation Through the Prism of Social Security." In: *Advances in Natural, Human-Made, and Coupled Human-Natural Systems Research, Volume 1*, edited by Svetlana G. Maximova, Roman I. Raikin, Alexander A. Chibilev, and Marina M. Silantyeva, 457-469. Springer, Cham. https://doi.org/10.1007/978-3-030-75483-9_42.

Kotliar, Dan M., and Elinor Carmi. 2023. "Keeping Pegasus on the Wing: Legitimizing Cyber Espionage." *Information, Communication & Society* 27 (8): 1499-1529. https://doi.org/10.1080/1369118X.2023.2245873.

Lamb, George William. 2025. "The UK and EU Security and Defence Relationship Post-Brexit." In: *The New Relationship between the United Kingdom and the European Union*, edited by Emmanuel Guinchard, and Carlo Panara, 251-318. Springer, Cham. https://doi.org/10.1007/978-3-031-70652-3_13.

Li, Hui, and He Bai. 2025. Network Control Message Protocol. In: Principle of Architecture, Protocol, and Algorithms for CoG-MIN: A Sustainably Ecological & Evolutionary Solution for Packet Network System. Springer, Singapore, pp. 197-228. https://doi.org/10.1007/978-981-96-3596-2_10.

Mizobuchi, Masaki. 2025. "The Other Active Fault Line: Israel, Iran, and the "Axis of Resistance"." In: *"Fragile Stability" as a Political Background of October 7: Current and Foreseeable Issues in the Israeli-Palestinian Conflict*, edited by Aiko Nishikida, Chie Ezaki, and Toshiya Tsujita, 205-220. Springer, Singapore. https://doi.org/10.1007/978-981-96-2587-1_12.

Möller, Dietmar P.F. 2023. Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation. In: Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Springer, Cham, pp. 273-303. https://doi.org/10.1007/978-3-031-26845-8_6.

Montasari, Reza. 2023. Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. In: Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity. Springer, Cham, pp. 7-25. https://doi.org/10.1007/978-3-031-21920-7_2.

Murphy, Graham J. 2024. Introduction: Strolling Through the Sprawl. In: William Gibson's "Neuromancer": A Critical Companion. Palgrave Science Fiction and

Fantasy: A New Canon. Palgrave Macmillan, Cham, pp. 1-20. https://doi.org/10.1007/978-3-031-56627-1_1.

Oladimeji, Saheed, and Sean Michael Kerner. 2023. "SolarWinds hack explained: Everything you need to know." *TechTarget, November 3, 2023*. Accessed January 21, 2025. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

Özdemir, Gloria Shkurti, and Ahmet Kayhan Yıldız. 2024. "Bringing Diplomacy to the Digital Age: The Implementation and Impact of Digital Diplomacy in the USA." In: *Digital Diplomacy in the OSCE Region: From Theory to Practice*, edited by Erman Akıllı, Burak Güneş, and Oğuz Güner, 113-123. Springer, Cham. https://doi.org/10.1007/978-3-031-50966-7_11.

Paulus, Alexandra. 2024. Introducing Key Concepts and the Analytical Framework. In: Building Bridges in Cyber Diplomacy: How Brazil Shaped Global Cyber Norms. Springer, Cham, pp. 39-61. https://doi.org/10.1007/978-3-031-60387-7_2.

Poghosyan, Benyamin. 2022. "US Policy in the South Caucasus Prior to and After the 2020 Karabakh War in the Context of the Evolving Regional and International Geopolitics." *Journal of Political Science: Bulletin of Yerevan University* 1 (3): 36-50. https://doi.org/10.46991/JOPS/2022.1.3.036.

Raghad, Sili Alsahli et al. 2024. "LUBB: Augmented Reality (AR) Application for Learning Transmission Control Protocol/Internet Protocol (TCP/IP) Model." In: *Intelligent Systems and Applications: Proceedings of the 2024 Intelligent Systems Conference (IntelliSys) Volume 2*, edited by Kohei Arai, 408-426. Springer, Cham. https://doi.org/10.1007/978-3-031-66428-1_25.

Reinhold, Thomas. 2024. From Cyberwar to Cyberpeace. In: Towards a Peaceful Development of Cyberspace: De-Escalation of State-Led Cyber Conflicts and Arms Control of Cyber Weapons. Springer Vieweg, Wiesbaden, pp. 51-72. https://doi.org/10.1007/978-3-658-43951-4_6.

Romano, Simon Pietro. 2024. "Cyber Warfare and Ethical Frontiers: Elevating Conflict to the Digital Frontline of Global Struggles." In: *Mind, Body, and Digital Brains. Integrated Science, vol 20*, edited by Flavia Santoianni, Gianluca Giannini, and Alessandro Ciasullo, 231-252. Springer, Cham. https://doi.org/10.1007/978-3-031-58363-6_15.

Singer, Peter W. and Allan Friedman. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know®. New York: Oxford University Press.

Singh, Niraj Kumar, and Sunil Bajeje. 2025. "Hacktivism or Cyber Warfare? Decoding the Motivations Behind Cyber Attacks Targeting Israel." In: *Artificial Intelligence Based Smart and Secured Applications. ASCIS 2024. Communications in Computer and Information Science, vol 2429*, edited by Sridaran Rajagopal, Kalpesh Popat, Divyakant Meva, Sunil Bajeja, and Pankaj Mudholkar, 206-232. Springer, Cham. https://doi.org/10.1007/978-3-031-86305-9_15.

Singh, Tarnveer. 2025. State-Sponsored Cyberattacks. In: Cybersecurity, Psychology and People Hacking. Palgrave Studies in Cyberpsychology. Palgrave Macmillan, Cham, pp. 147-150. https://doi.org/10.1007/978-3-031-85994-6_15.

Spînu, Natalia. 2020. Armenia Cybersecurity Governance Assessment. Geneva: DCAF - Geneva Centre for Security Sector Governance. Accessed January 21, 2025.

https://www.dcaf.ch/sites/default/files/publications/documents/ArmeniaCybersecurityGovernanceAssessment.pdf.

Stoddart, Kristan. 2022. Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In: Cyberwarfare: Threats to Critical Infrastructure. Palgrave Macmillan, Cham, pp. 351-399. https://doi.org/10.1007/978-3-030-97299-8_6.

Tabrizchi, Hamed, and Ali Aghasi. 2025. Fundamentals of Cybersecurity. In: Federated Cyber Intelligence: Federated Learning for Cybersecurity. Springer, Cham, pp. 45-74. https://doi.org/10.1007/978-3-031-86592-3_3.

Tavakkoli, Nasim et al. 2025. "From frontlines to online: examining target preferences in the Russia-Ukraine conflict." *International Journal of Information Security* 24 (64): 1-15. https://doi.org/10.1007/s10207-025-00981-w.

US Air Force. 2023. "Air Force Doctrine Publication 3-12, Cyberspace Operations." *February 1, 2023.* Accessed January 21, 2025. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf.

Uslu, Safa. 2024. "Data-Informed Diplomacy: Adapting to the Digital Age in International Relations and Implementation in the OSCE Region." In: *Digital Diplomacy in the OSCE Region: From Theory to Practice,* edited by Erman Akıllı, Burak Güneş, and Oğuz Güner, 155-166. Springer, Cham. Springer, Cham. https://doi.org/10.1007/978-3-031-50966-7_14.

Vitel, Philippe, and Henrik Bilddal. 2015. "French Cyber Security and Defence: An Overview." *Information & Security: An International Journal* 32 (1): 29-41. https://doi.org/10.11610/isij.3209.

Vogiatzoglou, Plixavra. 2025. "The EU's Quest for Digital Sovereignty: A Matter of Quantum Innovation?." *Digital Society* 4 (16): 1-19. https://doi.org/10.1007/s44206-025-00162-1.

Wade, Robert H. 2023. "Conflict Between Great Powers Is Back with Vengeance: The New Cold War Between the US and China Plus Russia." In: *The Political Economy of Emerging Markets and Alternative Development Paths*, edited by Judit Ricz, and Tamás Gerőcs, 13-35. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-20702-0_2.

Williams, Michael R., and Neil C. Rowe. 2025. "Russian Cyber Disinformation Campaigns and Possible Countermeasures." In: *Security and Management and Wireless Networks. CSCE 2024. Communications in Computer and Information Science, vol 2254*, edited by Kevin Daimi, Hamid R. Arabnia, and Leonidas Deligiannidis, 344-356. Springer, Cham. https://doi.org/10.1007/978-3-031-86637-1_25.