Pakistan Journal of Criminology
Vol. 16, No. 02, April—June 2024 (309-326)

The Use of Means of Military Diplomacy in Providing Information Security as a Peacebuilding Factor

Viktor Shemchuk[1], Andrii Bozhkov[2], Serhii Naumiuk[3],
Alexander Rusnak[4] &Mykola Shilin[5]

Abstract

The research aims to determine the role of military diplomacy in providing information security as a key factor in building peace through the identification of key measures to counter information threats in the digital environment. The research employed the following methods: content analysis, rating analysis, and survey results processing. As a result of the conducted research, the place of digital diplomacy was determined concerning military diplomacy as a special form of its implementation to provide information security. The security of cyber-physical systems has been proven to be one of the most important approaches to data protection in military diplomacy because, among other things, the security of critical infrastructures depends on it. The research findings can be used by diplomatic service officers to increase the effectiveness of military diplomacy in the digital environment by implementing the proposed measures and directions in their activities.

Keywords: National security, information security, military security, military diplomacy, cyber-physical systems, peace building

Introduction

The problem of providing information security becomes especially urgent and strategically important in the digital age when technological achievements are developed at a particularly high level. As an important tool of influence and interaction at the international level, military diplomacy occupies a special place

[1] The author is a Doctor of Juridical Sciences, Professor of the Department of Theory of Law, Constitutional and Private Law, Faculty No.1 of the Institute for the Training of Specialists for Units of the National Police, Lviv State University of Internal Affairs, Ukraine. He can be reached at vshemchuk58@gmail.com

[2] The author is a Chief of the International Cooperation Department, Interregional Academy of Personnel Management, Ukraine. He can be reached at a.bozhkov.maup@gmail.com

[3] The author is a Candidate of Law Sciences, Professor of the Special Chair, Training and Research Centre of State Security, National Academy of the Security Service of Ukraine, Ukraine. He can be reached at Snaum489@ukr.net

[4] The author is a Doctor of Law, Professor of the Department of Counterintelligence, National Academy of the Security Service of Ukraine, Ukraine. He can be reached at a_rusnakk@yahoo.com.ua

[5] The author is a Doctor of Law, Professor of the Educational and Research Institute of State Security, National Academy of Security Service of Ukraine, Ukraine. He can be reached at Mkshl1986@gmail.com

in providing information security. It is not only a tool for resolving conflicts and peace building but also actively protects national interests and national security. Therefore, it is important to understand the information security measures that military diplomacy offers, as well as their applications.

Several researchers studied the relationship between diplomacy and providing information security (Kim, 2022; Kalina et al., 2022; Kadlecová et al., 2020; Bendiek & Kettemann, 2021). Such studies do not often use the term "military diplomacy" directly but describe certain conflict situations. Digital diplomacy or cyber diplomacy is often used when research concerns information security issues (Goldman, 2020; Semenets-Orlova et al., 2022; Manantan, 2021). Studying the concept of cyber diplomacy (Barrinha & Renard, 2020), as well as emphasising its role in countering informational threats generated by cyberspace (Broeders et al., 2023). Avramenko (2023) used the Ukrainian case, noting that the need to repel information attacks by the Russian Federation (RF) was the impetus for developing digital diplomacy in the country. The Russian Federation launched a large-scale campaign in cyberspace to legitimise or hide its criminal activities. External military aggression determined the need to develop Ukrainian diplomacy to restore peace, which also expanded into the digital space. The potential of digital diplomacy gradually began to be used to form a positive image of the country in the international arena and increase the informational presence of Ukraine in the media space of foreign audiences.

So, because of the foregoing and taking into account that the object of the article is information security, the key research vector is the study of the influence of military diplomacy in the information environment. Accordingly, it is proposed that the focus be on digital means of military diplomacy to provide information security. Therefore, special attention is paid in this study to digital diplomacy as a form of military diplomacy to provide information security and peacebuilding.

The study aims to determine the role of military diplomacy in providing information security as a key factor in building peace by identifying key measures to counter information threats in the digital environment.

Research objectives:

- Determine the place of digital diplomacy relative to military diplomacy as a special form of its implementation for providing information security;
- Determine the current state of providing information security in Ukraine according to individual indicators;
- Describe the directions of military diplomacy in the digital environment aimed at providing information security.

Methodology

Research design

The first stage of the study involved determining the place of digital diplomacy with military diplomacy as a special form of its implementation for providing information security. An approach is proposed in which digital diplomacy is interpreted as a form of implementation of military or other areas of diplomacy and not as a separate area of diplomacy.

The second stage described the identified directions of countering threats to information security through military diplomacy in the digital sphere. The first of them is countering information threats (disinformation campaigns and cyber security threats). The related measures are proposed, and the current state of Ukrainian media literacy and the position of Ukraine according to the Cyber Security Index and the Digital Development Level are also characterised. The second direction is providing information security through communications. Special attention is paid to social networks. The indicators that show the popularity of key information sources and social networks for Ukrainians are given according to the percentage of respondents who use them. An example of the spread of manipulation using social networks is given, and the consequences are described. The third direction is countering threats to information security through military diplomacy in the digital environment by implementing basic preventive and intelligence measures.

The third stage of research concerns the identification of the features of the security of cyber-physical systems as an approach to data protection in the field of military diplomacy. Among other things, the security of critical infrastructures depends on it. The key elements of this approach, as well as the most used technologies, are identified.

The fourth stage of the study involved reviewing international experience in providing information security through military diplomacy. The main measures taken in this area by such countries and organisations as NATO, the USA, the EU, and China are discussed.

Sample

Ukraine is an example of this study, given the relevance of providing information security during wartime for this country. The large-scale invasion of the Russian Federation on the territory of Ukraine was preceded by an information war on the part of the aggressor, which stimulated the development of diplomacy in the country. Therefore, the Ukrainian case is a good example of studying the role of military diplomacy in providing information security. NATO, the USA, the

EU, and China were taken as countries and organisations that demonstrate successful examples in the context of the issue under research.

Methods

The research employed the method of content analysis to study the content of several regulatory documents. The rating method was used to analyse the level of cyber security in the country through the National Cyber Security Index and the Digital Development Level as of September 1, 2023. The results of respondent surveys were also processed to determine the media literacy level of Ukrainians and the most popular sources of information and social networks.

Literature review

The researchers often do not distinguish military diplomacy, considering it a part of diplomacy. Providing information security also does not have a defined place in the diplomatic sphere. For example, Trofymenko and Trofymenko (2020) considered countering negative informational influence (disinformation campaigns, cyberattacks) as a component of the public diplomacy model.

Distinguishing the functions of countering disinformation or ensuring information security as part of different types of diplomacy leads to uncertainty and inconsistency. In the author's opinion, these functions correspond to the category of digital diplomacy. Digital diplomacy can be applied in various spheres, including the military. Therefore, the provision of information security will be analysed through the prism of military diplomacy in the digital environment. Tsivatyi (2023) reflected this approach, noting that efficiency in information security can be achieved through institutional interaction in diplomatic communication, public administration, politics, and international relations. In turn, the digital diplomacy cluster is the institutional basis of the current model of diplomacy. Kubko and Potapchuk (2023) define digital (electronic) diplomacy as the ability to use ICT and the Internet to support and implement foreign policy goals. Researchers note that until recently, diplomacy, in general, was a relatively closed sphere of activity. However, it gradually moved into the public sphere with the development of new technologies. This was facilitated by the inclusion of communication in the sphere of diplomacy "into the global context of network interaction". So, we can conclude that digital diplomacy is not a separate type of diplomacy. It is a new form of implementation in other spheres — economic, political, military, etc.

However, digital diplomacy is not reduced to the public sphere only. As Rashica (2019) noted, in addition to public diplomacy and social media, activities in the field of digital diplomacy include diplomatic negotiations, political initiatives and crisis management. These activities are significantly dependent on digital technologies. The researchers note that, despite digital diplomacy's unconditional and numerous advantages (speed of communication, reduction of costs, strengthening of international relations), it is characterised by significant risks associated with hacking and the spread of extremist and terrorist ideologies. In this regard, some researchers urge the concept of cyber diplomacy. According to Attatfa et al. (2020), cyber diplomacy is the use of diplomatic tools to solve problems arising in the global use of cyberspace. The military dimension is one of the dimensions of cyber diplomacy. Lancelot (2020) highlights the problem that many critics do not see cyberwar as a threat to national security. The researcher emphasises that cyber diplomacy is at the very centre of politics. It cannot be defined as diplomacy in cyber space only because it is the essence of conducting a state defence strategy in the era of cybernetics. Cyber security is considered in several studies as an integral component of national security, especially in the context of providing cyber security of critical infrastructures (Chowdhury & Gkioulos, 2021; Dawson et al., 2021; de Soto et al., 2020; Viganò et al., 2020).

Szostek (2020) considers the case of Ukraine in his study on the search for an answer to what happens to public diplomacy in information warfare. The researcher notes that the media projects supported by Western governments to attract the Ukrainian audience, as well as the attraction of the international audience by the Ukrainian mass media, are considered a response to the information war unleashed by the Russian Federation. In this context, the researcher notes that discussions about state communication with representatives of other countries are conducted more and more often not using public diplomacy but by the language of information warfare.

As can be summarised from the literature review, there are many approaches to the interpretation and classification of diplomacy. Military diplomacy is often seen as one of the dimensions of diplomacy. In addition, it becomes clear that today, diplomacy (including military) is presented in two key forms: traditional and digital. Cyber diplomacy can be separately distinguished from digital diplomacy, which is intended to counter cyber threats. Given the aim set in the research to ensure information security, special attention is paid to the digital form of military diplomacy.

Results

Digital diplomacy is a special form of implementation of military diplomacy to provide information security

Information security, military security, and cyber security are components or directions of national security. They serve a single purpose - protecting the national interests of the state. The activity of the diplomatic service involves primarily the protection of such interests through diplomatic means. In the context of the research, the means of public diplomacy are of greatest interest, namely, the means provided for one of the key areas — digital diplomacy. The Doctrine of Information Security of Ukraine (Verkhovna Rada of Ukraine, 2017) states that the development of public diplomacy (together with cultural and digital) is one of the priorities of state information policy. The formation and implementation of Ukraine's public diplomacy strategy should be entrusted to the Ministry of Foreign Affairs of Ukraine.

The Public Diplomacy Strategy of the Ministry of Foreign Affairs of Ukraine (2021) for 2021-2025 (hereinafter — the Strategy) states that the work of public diplomacy subjects in the field of digital diplomacy is considered through the following aspects: 1) interaction with international digital platforms for improving Ukraine's image and protecting national security; 2) use of digital tools for organising events and projects in the field of public diplomacy; 3) active use of social networks and interaction with online communities for shaping a positive image of Ukraine and protecting national interests in the world.

Analysing the content of the Strategy, it can be noted that digital diplomacy is the only direction of public diplomacy, which is tasked to secure national interests. This indicates a close connection between digital diplomacy and national, in particular, information security. It is worth noting that the development of digital diplomacy in Ukraine was powerfully driven by the Russian Federation's information attacks. So, in the context of the study, it is appropriate to turn to the key means of military diplomacy in the digital environment aimed at providing information security, dividing them into several directions.

Directions for countering threats to information security using military diplomacy in the digital environment

The first direction considers means of countering information threats, primarily such as disinformation campaigns and threats to cyber security. Countering the spread of disinformation includes not only refuting fakes, manipulations, exposing propaganda, and blocking certain sources of information. An important way to counter disinformation using military diplomacy in the digital environment is by conducting educational campaigns and activities to increase the population’s awareness and media literacy. This promotes the development of critical thinking and fact-checking skills. Based on the analytical report on the results of the Media Detector study, the Media Literacy Index of Ukrainians increased significantly after the start of the full-scale invasion (Figure 1).

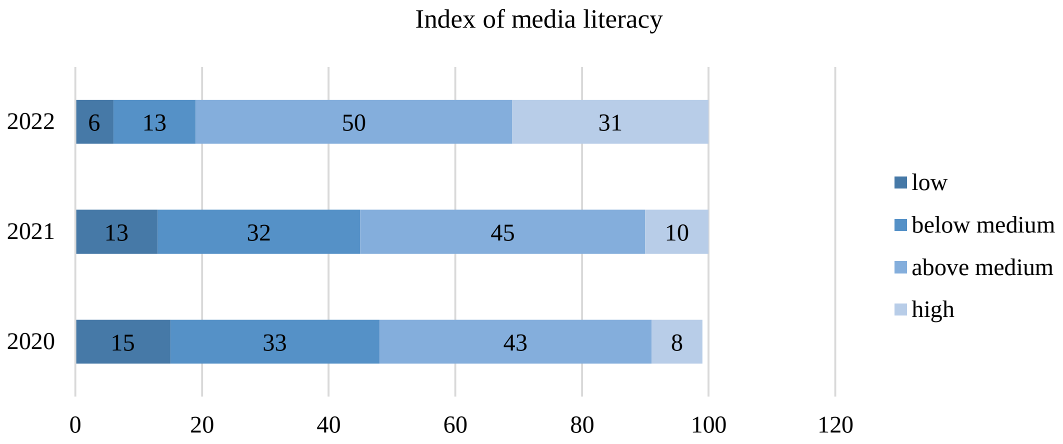

Figure 1. Media Literacy Index of Ukrainians for 2020-2022 (built by the author according to Naumova (2023))

The Media Literacy Index considers four sub-indices: understanding, usage, digital competence, and distorted media content. The results presented in Figure 1 show that before the full-scale invasion (as of 2021) 55% of Ukrainians had above medium and high level of media literacy, after it (as of 2022) – 81%. An important role in this progress was probably played by educational campaigns and information dissemination through various sources on the part of mass media and government officials (including the diplomatic service). Also important is citizens’ desire to receive reliable information when the need for it arises, especially acutely.

The threat of cyberattacks is no less important than the problem of spreading disinformation. In this case, military diplomacy in the digital environment relies even more on the use of information technology. Ukraine ranks 24th in the world on the Cyber Security Index (Figure 2) with a score of 75.32, but lags behind significantly in digital development with a score of 55.96.

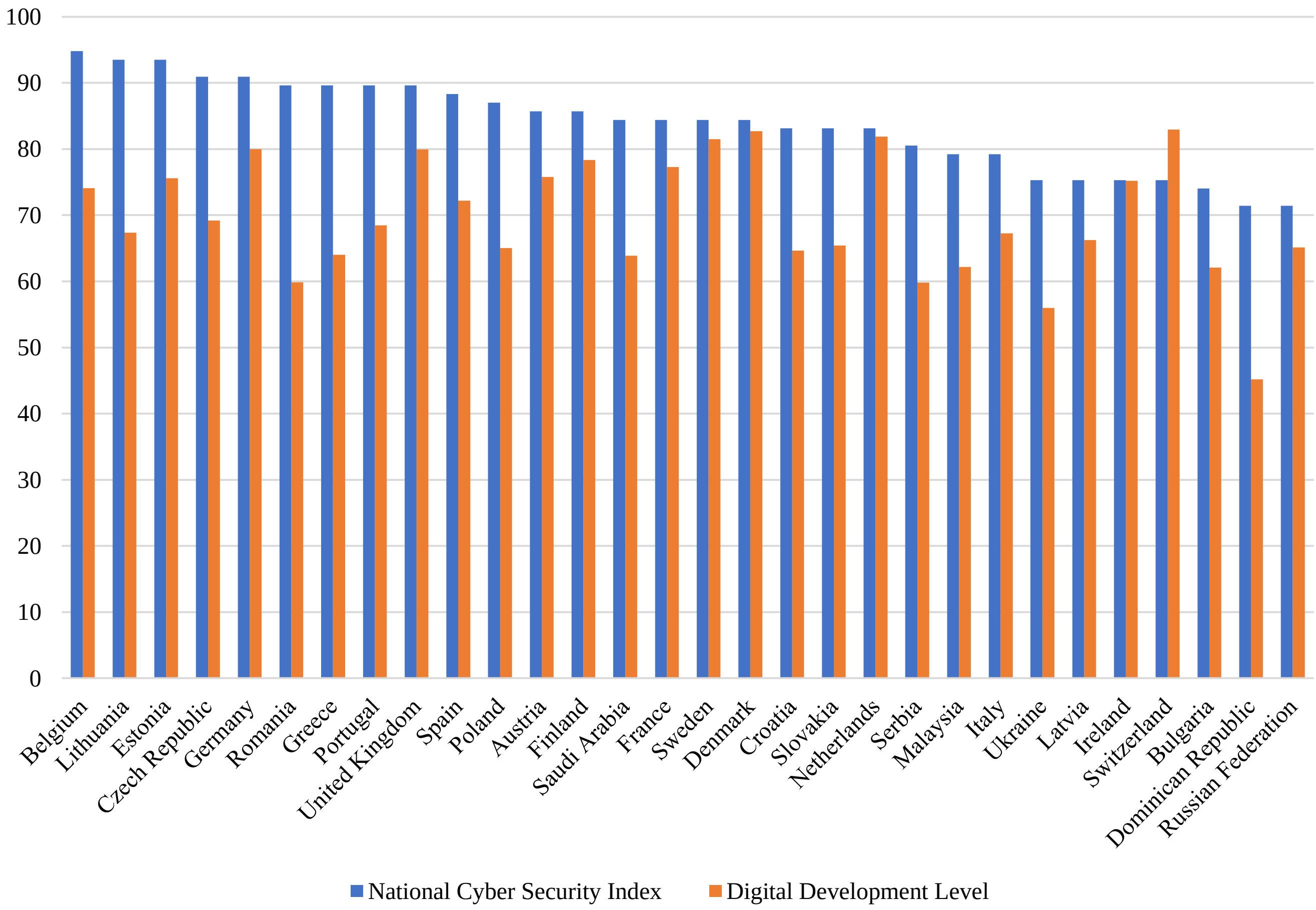

Figure 2. National Cyber Security Index and the Digital Development Level as of September 1, 2023 (for 30 leading countries) (built by the author according to National Cyber Security Index (2023))

The diplomatic service can implement direct countermeasures against cyber threats with the involvement of technology specialists and/or technology companies. Direct countermeasures mean using specific innovative methods and technologies, such as antivirus software, firewalls, intrusion detection and prevention systems, data encryption algorithms, multiple authentication, and specialised systems to ensure the safety of critical infrastructure.

In addition to technological measures, the diplomatic service can counter cyber threats by purely diplomatic means, including the conclusion of international agreements, development of international norms and standards of behaviour in cyberspace, conducting diplomatic negotiations, organisation and participation in international forums and conferences, making diplomatic statements or appeals, creation of international working groups involving experts, conducting information and educational campaigns, etc.

The second direction of military diplomacy in the digital environment, which is aimed at ensuring information security, can be revealed through measures in the field of communications. First, this activity provides for disseminating reliable information about the conflict and ensuring the awareness of as many citizens as possible, particularly from other countries. The war of the Russian Federation against Ukraine became the first full-scale cyber war — both because of the spread of hacking and the possibility of watching it online in real time (Avramenko, 2023). According to research by Ipsos (2022), 70% of respondents from 27 different countries of the world followed the war in Ukraine. At the same time, according to the evidence of the Eurobarometer, more than 75% of the surveyed citizens of the USA, the EU, and Great Britain observe events through social networks (Kovach, 2022). According to a survey conducted by Detector Media (Chorna, 2023), social networks in Ukraine are the leader among all sources of information about the war (Figure 3). Figure 4 shows which social networks are the most popular.

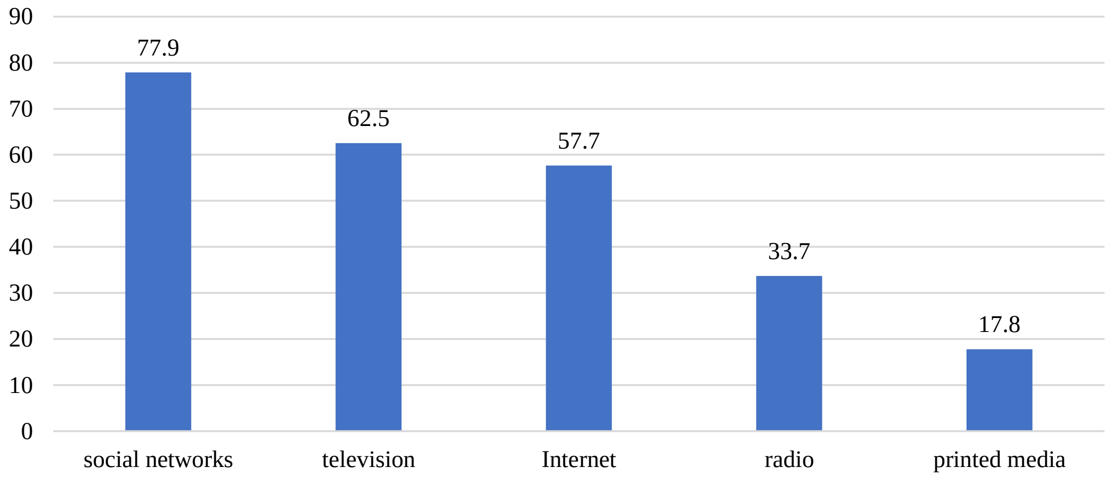

Figure 3. Distribution of the Ukrainian audience by sources of information (built by the author according to Chorna (2023))

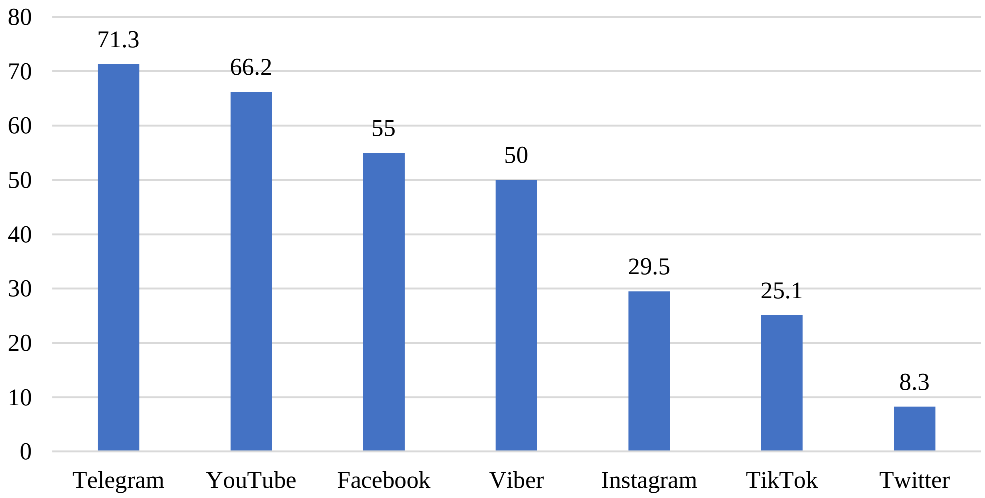

Figure 4. Distribution of the Ukrainian audience by the use of specific social networks (built by the author according to Chorna (2023))

The diplomatic work of Ukrainian politicians, particularly President V. Zelenskyi and Minister of Digital Transformation M. Fedorov, is worth noting. Politicians use social networks for quick communication with politicians, company heads, and citizens.

The third direction of military diplomacy in the digital environment aimed at providing information security involves preventive and intelligence measures. It includes information counterintelligence, electronic intelligence and communication interception, control of information platforms, etc. This means that this direction considers not only the need to defend against negative informational influence from the enemy but also the need to convey facts to the general public. Also, the direction includes actions that can contribute to the prevention of further attacks, as well as actions aimed at obtaining information that can provide certain military advantages and restore peace.

Security of cyber-physical systems as a priority approach to data protection in the field of military diplomacy

Some technological clusters that can be used in military diplomacy to provide information security were indicated in the previous subsection of the work. This subsection offers a more detailed study of cyber-physical security or security of cyber-physical systems as an approach to data protection. Cyber-physical security is associated with cyber security network technologies and information security management systems mentioned earlier but may overlap with other areas of cyber security. The important role of cyber-physical security is to ensure the reliable and continuous operation of critical infrastructures. This is necessary during a military conflict and in restoration and peacebuilding, which determines the choice of this field in military diplomacy.

The cyber-physical security system may contain several elements, in particular:

1) systems for monitoring and detecting introductions designed to detect anomalies and threats in physical and digital systems. Examples: Splunk, IBM QRadar, or ELK Stack.

2) Integrated physical and cyber security systems – combine physical and cyber security methods (e.g. access control and intrusion detection). Examples: Genetec Security Centre or CNL Situational Awareness.

3) Network infrastructure protection systems – include such protections as firewalls (for example, Cisco ASA or Palo Alto Networks), VPN (Virtual Private Network), encryption, and various intrusion detection systems.

4) Physical security systems — include surveillance cameras, motion sensors, various sensors, systems for authentication based on biometric data (in particular, MorphoWave or HID Global), etc.

5) Hardware attack prevention systems are designed to provide security for equipment and microcircuits. These include TPM (Trusted Platform Module), such as TPM 2.0, and HSM (Hardware Security Module), such as Thales nShield or Gemalto SafeNet (IBM, 2023).

6) Systems for providing security of critical infrastructure from physical and cyber threats. In this context, it is possible to cite such examples as SCADA (Supervisory Control and Data Acquisition) designed for monitoring and controlling systems (in particular, Siemens WinCC or Schneider Electric EcoStruxure) (Inductive automation, 2018) and DNP3 (Distributed Network Protocol) — a set communication protocols used between components of process automation systems.

7) Penetration testing systems are designed to identify and eliminate weaknesses in systems (Metasploit, Burp Suite, or Nmap) (IBM, 2023).

International experience

In addition to the issues discussed in the previous sections, it is important to consider the successful international experience of ensuring information security through military diplomacy. This will allow us to consider the studied issue at the global level.

NATO. The North Atlantic Treaty Organization is actively developing and implementing cyber defence standards, particularly in military information systems. Besides, the participation in annual exercises, such as Locked Shields, is also worth noting in the context of NATO. Locked Shields is organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) to improve cyber security expertise to protect the nation's IT systems and critical infrastructure from real-time attacks (CCDCOE, 2023).

USA. In the United States, government initiatives have created CISA — the Cybersecurity and Infrastructure Security Agency (CISA, 2023). The high importance of cooperation with the private sector on cyber security issues in the context of the USA should be noted.

EU. In the EU, Europol established the European Cybercrime Centre (EC3) to improve the effectiveness of law enforcement response to cybercrime in the union. This improves the protection of European citizens, businesses, and governments against criminals in cyberspace (Europol, 2023). Moreover, the General Data Protection Regulation (GDPR) was introduced, which contains provisions for processing personal information of data subjects in the EU.

Israel. In Israel, there is Unit 8200 for radio-electronic intelligence, which is engaged, among other things, in collecting and decoding radio-electronic information and other operations. In addition, the country cooperates with private cyber companies, which allows the use of high-tech protection tools.

China. China is another example of countries that pays significant attention to cyber defence at the state level. This is implemented through large-scale cyber military exercises and strict regulation of cyber security to ensure national security.

Discussion

The study aimed to determine the role of military diplomacy in providing information security as a key factor in building peace through the identification of key measures to counter information threats in the digital environment. Following the set goal, three directions of providing information security and countering information threats using military diplomacy in the digital space were identified during the research:

1. The first direction of providing information security using military diplomacy in the digital space in the author's work is countering information threats: disinformation and cyber threats. Trofymenko and Trofymenko (2020) also distinguish countering hostile disinformation campaigns as a direction of activity of the diplomatic service that digital diplomacy is a component of public diplomacy. As regards the practical part, in particular, the author's statement about the importance of educational campaigns and increasing media literacy in countering disinformation, the work of Szostek (2020) is worth noting. The researcher indicated that communication can be used as a weapon to achieve the

planned impact. Second, the audience is vulnerable and, therefore, communicates with the enemy. Third, victory in the information war implies success in coercive new disclosure of certain facts to citizens — in other words, and it is necessary to make the latter believe in information beneficial to a certain party.

The author stated that the role of cyber diplomacy in the military sphere is significant, which other researchers support. Attatfa et al. (2020) deal with the dimensions of cyberdiplomacy and distinguish, among others, the military dimension. However, some researchers emphasise the lack of international rules for warfare in cyberspace as a serious problem. Lancelot (2020) notes that cyberspace is embedded in nation-state international relations, and it is not going away. The researcher emphasises that there are very few legal consequences for states waging cyberwar.

2. The second direction of military diplomacy in the digital sphere aimed at providing information security is revealed in the author's research through measures in the field of communications. Special attention is paid to the role of social networks. Kubko and Potapchuk (2023) also note that diplomacy in Ukraine uses such tools as creating accounts for diplomatic missions on Twitter, Facebook, and Instagram and maintaining accounts by political figures and diplomats on social networks. Rashica (2019) also emphasises using social networks in digital diplomacy. Thus, an increasing number of researchers confirm the importance and significance of social networks in diplomacy and politics.

3. The third direction of military diplomacy in the digital sphere, as determined in the author's article, is aimed at providing information security through preventive intelligence measures. Tsivatyi (2023) distinguished specific technologies that can be useful in applying the measures determined by the author. In particular, this is processing large data sets and artificial intelligence.

In addition to the mentioned directions, the study emphasised providing critical infrastructure security. This approach is widely covered by de Soto et al. (2020), who particularly study cybersecurity in constructing and protecting critical infrastructures. Viganò et al. (2020) emphasise the importance of cyber security of critical infrastructures in the national security system. This proves the author's appropriateness in considering cyber security issues within the scope of research on providing information security using military diplomacy. Considering the cybersecurity of critical infrastructures as a national and international security topic, Dawson et al. (2021) identified key threats to such security. The recognition of CISA's role in ensuring cyber security at the state level is common in the studies. Chowdhury and Gkioulos (2021) explore approaches to delivering cybersecurity training to protect critical infrastructure. The international experience presented in the author's research testifies to the wide use of various approaches to cyber security training by such countries and organisations as China and NATO.

Conclusions

The means of military diplomacy in the digital sphere can play a significant role in ensuring information security and further development of the conflict. The practical achievements of the research include the main directions of countering threats to information security using military diplomacy in the digital environment. The first direction considers means of countering information threats, primarily such as disinformation campaigns and threats to cyber security. The second direction of military diplomacy in the digital environment aimed at providing information security is revealed through measures in the field of communications. The third direction of military diplomacy in the digital sector aimed at providing information security includes preventive intelligence measures. The novelty of the study is the clarification of the place of digital diplomacy concerning military diplomacy as a special form of its implementation for the provision of information security, as well as the definition of the main directions of military diplomacy in the digital environment aimed at providing information security. Further research should focus on proposals for improving international law in determining responsibility for cyber warfare and disinformation.

Recommendations

Based on the results of the research, some recommendations can be formulated regarding the use of means of military diplomacy in ensuring information security as a factor in building peace:

- conducting educational campaigns and events aimed at increasing awareness and media literacy;
- application of information technologies to counter cyber attacks;
- use of diplomatic means to counter cyber threats;
- dissemination of reliable information about the conflict and ensuring awareness of the largest possible circle of citizens, in particular from other countries;
- conducting preventive intelligence measures;
- ensuring cyber-physical security through intrusion detection and monitoring systems and other instruments.

References

Attatfa, A., Renaud, K., & De Paoli, S. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science*, 176, 60-69. https://doi.org/10.1016/j.procs.2020.08.007

Avramenko, M. (2023). Ukrainian digital diplomacy in conditions of war. *May Studies: History, Political Science, International Relations*, 8, 110-113. Retrieved from https://jts.donnu.edu.ua/index

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs*, 96(3), 749-766. https://doi.org/10.1093/ia/iiz274

Bendiek, A., & Kettemann, M. C. (2021). Revisiting the EU cybersecurity strategy: a call for EU cyber diplomacy. SWP. https://doi.org/10.18449/2021C16

Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too close for comfort: Cyber terrorism and information security across national policies and international diplomacy. *Studies in Conflict & Terrorism*, 46(12), 2426-2453. https://doi.org/10.1080/1057610X.2021.1928887

CCDCOE. (2023). Locked Shields. Retrieved from https://ccdcoe.org/exercises/locked-shields/

Chorna, O. (2023). “Opora”: The main source of information for almost 80% of Ukrainians is social networks. *PO «Media Detector»*. Retrieved from https://detector.media/infospace/article/213998/2023-07-10-opora-osnovnym-dzherelom-informatsii-mayzhe-80-ukraintsiv-ie-sotsialni-merezhi/

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

CISA. (2023). About CISA. Retrieved from https://www.cisa.gov/about

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*, 26(1), 69-75. https://doi.org/10.2478/raft-2021-0011

de Soto, B. G., Georgescu, A., Mantha, B., Turk, Ž., & Maciel, A. (*2020*). Construction cybersecurity and critical infrastructure protection: Significance, overlaps, and proposed action plan. *Preprints.* https://doi.org/10.20944/preprints202005.0213.v1

Europol. (2023). European Cybercrime Centre - EC3: Combating crime in a digital age. Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Goldman, E. O. (2020). From reaction to action: Adopting a competitive posture in cyber diplomacy (Fall 2020). *Texas National Security Review*, 3(4). http://dx.doi.org/10.26153/tsw/10950

IBM. (2023). Build workfows you can trust. Retrieved from https://www.ibm.com/

Inductive automation. (2018). SCADA: Supervisory Control and Data Acquisition. What is SCADA, Who Uses it and How SCADA Has Evolved. Retrieved from https://inductiveautomation.com/resources/article/what-is-scada

Ipsos. (2022). Global public opinion about the war in Ukraine. Retrieved from https://www.ipsos.com/en-us/news-polls/war-in-ukraine-april-2022

Kadlecová, L., Meyer, N., Cos, R., & Ravinet, P. (2020). Cyber security: Mapping the role of science diplomacy in the cyber field. In M. Young, T. Flink, & E. Dall (Eds.), *Science Diplomacy in the Making: Case-based insights from the S4D4C project* (pp. 62-96). *S4D4C.* Retrieved from https://www.s4d4c.eu/wp-content/uploads/2020/03/D3.2_3_Cyber_final.pdf

Kalina, I., Khurdei, V., Shevchuk, V., Vlasiuk, T., & Leonidov, I. (2022). Introduction of a corporate security risk management system: The experience of Poland. *Journal of Risk and Financial Management*, 15(8), 335. https://doi.org/10.3390/jrfm15080335

Kim, S. (2022). The Inter-network Politics of Cyber Security and Middle Power Diplomacy: A Korean Perspective. In S. Lee, & S. Kim (Eds.), *Korea's Middle Power Diplomacy: Between Power and Network* (pp. 97-123). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-76012-0_6

Kovach, A. (2022). Ukrainian digital diplomacy: the information front of the state in social networks. *Analytical Center ADASTRA*. Retrieved from https://adastra.org.ua/blog/ukrayinska-cifrova-diplomatiya-informacijnij-front-derzhavi-v-socialnih-merezhah

Kubko, V. P., & Potapchuk, A. (2023). Digital diplomacy as a tool of foreign policy. In O. S. Sainchyn, A. E. Prylutska, O. V. Hehechkori, I. M. Chistyakova, & H. V Ozernyuk (Eds.), *Materials of the Round Table: Cross-Border Cooperation in the Conditions of Armed Conflicts* (pp. 43-46). Odesa. Retrieved from http://dspace.op.edu.ua/jspui/bitstream/123456789/13880/1/27_01_2027_%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BA%D0%B0%D1%80%D0%B4%D0%BE%D0%BD%D0%BD%D0%B5_%D1%81%D0%BF%D1%96%D0%B2%D1%80%D0%BE%D0%B1%D1%96%D1%8

2%D0%BD%D0%B8%D1%86%D1%82%D0%B2%D0%BE_%D0%B7%D0%B1%D1%96%D1%80%D0%BA%D0%B0_%D1%82%D0%B5%D0%B7_%D0%BA%D1%80%D1%83%D0%B3%D0%BB%D0%BE%D0%B3%D0%BE_%D1%81%D1%82%D0%BE%D0%BB%D1%83.pdf

Lancelot, J. F. (2020). Cyber-diplomacy: Cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, 4(4), 240-254. https://doi.org/10.1080/23742917.2020.1798155

Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, 75(4), 432-459. https://doi.org/10.1080/10357718.2021.1926423

Ministry of Foreign Affairs of Ukraine. (2021). Public diplomacy strategy of the Ministry of Foreign Affairs of Ukraine for 2021-2025. Retrieved from https://mfa.gov.ua/storage/app/sites/1/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%97/public-diplomacy-strategy.pdf

National Cyber Security Index. (2023). Archived data from 01.09.2023. Retrieved from https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

Naumova, M. (*2023*). Media literacy index of Ukrainians: 2020-2022 (Analytical report based on the results of a comprehensive study). *PO «Media Detector*. Retrieved from https://detector.media/infospace/article/210210/2023-04-18-indeks-mediagramotnosti-ukraintsiv-2020-2022-povna-versiya/

Rashica, V. (2019). Digital diplomacy: aspects, approaches and practical use. *European Perspectives − International Scientific Journal on European Perspectives*, 10(17), 23-41. Retrieved from https://www.europeanperspectives.org/storage/41/PDF_04_2019.pdf#page=23

Semenets-Orlova, I., Rodchenko, L., Chernenko, I., Druz, O., Rudenko, M., & Poliuliakh, R. (2022). Requests for public information in the state administration in situations of military operations. *Anuario De La Facultad De Derecho. Universidad De Extremadura*, 38, 249-270. https://doi.org/10.17398/2695-7728.38.249

Szostek, J. (2020). What happens to public diplomacy during information war? Critical reflections on the conceptual framing of international communication. *International Journal of Communication*, 14, 1-21. Retrieved from https://ijoc.org/index.php/ijoc/article/view/13439

Trofymenko, M., & Trofymenko, A. (2020). Public diplomacy in the countries of Central and Eastern Europe: Experiences for Ukraine. In O. Bogdanova, & A. Makarychev (Eds.), *Baltic-Black Sea Regionalisms: Patchworks and*

Networks at Europe's Eastern Margins (pp. 235-243). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-24878-9_15

Tsivatyi, V. H. (2023). Information security and cross-border diplomacy of Ukraine in the context of the transformation of the system of international relations and the implementation of the Eastern Partnership program: institutional and international political discourses. In *Collection of Materials of the Internet Conference: Ukraine in Eastern Coordinates Partnerships: The Search for Geopolitical Priorities Through a National Prism Security* (pp. 60-64). Lviv: Lviv Polytechnic Publishing House. Retrieved from https://lpnu.ua/sites/default/files/2021/pages/14947/thesisofconference2023-2-1-1.pdf#page=60

Verkhovna Rada of Ukraine. (2017). Document N0 016525-16. Decision About the Information Security Doctrine of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/n0016525-16#Text

Viganò, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of critical infrastructure. *The Ethics of Cybersecurity*, 21, 157-177. Retrieved from https://library.oapen.org/bitstream/handle/20.500.12657/47324/9783030290535.pdf?sequence#page=169