THE DEVELOPMENT OF INTERNATIONAL LAW AND PUBLIC INSTITUTIONS IN THE CONTEXT OF CYBERSECURITY

[a]DIANA KIRIKA, [b]NADIIA DEMCHYK, [c]NADIIA SKLIAR, [d]LIDIIA VDOVICHENA, [e]OLEKSANDRA GAYEVAYA

[a]Higher Educational Institution "Podillia State University" Kamianets-Podilskyi, Ukraine
[b]National Academy of the State Border Guard Service of Ukraine named after Bohdan Khmelnytsky, Khmelnytsky, Ukraine
[c]Kryvyi Rih Educational and Scientific Institute, Donetsk State University of Internal Affairs, Ukraine
[d]Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine
[e]National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
email: [a]dkirika7@gmail.com, [b]demnpet@ukr.net, [c]test20@ukr.net, [d]l.vdovichena@chnu.edu.ua, [e]sa0613@ukr.net

Abstract: This study aims to substantiate the theoretical and applied principles of the current international law features' research and assessment of its impact on cyberspace. Regarding the study results we found that the EU countries are divided into three groups: highly developed, providing high rates of international law implementation to counter cyberthreats and ensure state stability; mid-developed countries with adequate capacity and capability to ensure high rates of international law implementation to counter cyberthreats and ensure state stability, but their institutional and legal mechanism is imperfect; developing countries and those completing the process of harmonizing national legislation with international law, which slows down countering cyberthreats and does not contribute to greater state stability.

Keywords: Globalization, International Law, Cyberspace, Legal Obligations, Law Principles, Cyber-Attacks.

1 Introduction

International instability of socio-economic and socio-political origins aggravates the processes of new challenges, threats, and dangers to global and national security. Globalization and geopolitical transformations violate certain countries' interests and lobby them concerning others. As a result, interstate relations are shaped by the constant committing of malicious cyber operations. It is obvious that cyber threats increase pressure on security issues, and studying international legal globalization requires increased attention to harmonizing national law with international norms. It happens because, at the present stage, ensuring human rights and resolving interstate conflicts are beyond the individual capabilities of the state and act as strategic priorities of each country, the decline of which stability is fraught with state sovereignty and territorial integrity.

Furthermore, internationalization has led to the emergence of intergovernmental organizations and transnational corporations, which produce norms of law at the international and regional levels. International law is the primary regulator of international relations and is characterized as a particular legal system. It includes social and political principles and legal norms that define relations between actors and international organizations, including cyberspace. Considering the outlined tendencies, the research problem of current international law specifics and its influence on cyberspace acquires particular importance.

2 Literature review

The new world order is being formed in the unstable conditions of international legal relations globalization. Intensification of digital technology development has created an interactive information environment (virtual space), carrying out its functions with the help of computer systems, enabling the implementation of social relations and communications using global data networks. Al-Mahrouqi et al. (2015) call such an interactive information environment cyberspace and consider it as a network of interconnected electronic communication channels, functioning through the transnational organization of cyberspace networks based on privacy and data security.

The acceleration of cyber capabilities development and the increasing illegal activities in the virtual environment make it necessary to regulate the legal relations of states in cyberspace through international law. In addition, Valori (2022) believes that the intensification of cyberspace development poses significant threats to state institutions, businesses, and the population, which are manifested in the protection of personal data and, at the same time, stimulates the intensification of innovation in software development, which requires adequate legal defense at the international level. In this context, Vihul (2018) argues that cyberspace is subject to the principles of sovereignty, jurisdiction, and the prohibition against interfering in other countries affairs, including using force. The scientist suggests compliance with international laws, norms, and treaties to resolve such problematic issues and allows countries to apply countermeasures against malicious cyberactivity to deescalate unauthorized situations legally. A similar position is held by Moulin (2020), who challenges the use of such international law norms as sovereignty and prohibition on the use of force and partially levels them to the extent that they apply to cyberspace. At the same time, it increases the relevance of the non-interference principle, which indirectly regulates cyber threats and provides a distinction between the concepts of territoriality and cyberspace militarization.

According to Bargiacchi (2020), legislative resolution of these problems can be achieved through an effective mechanism of international law, whose academic works raise the problematic aspects of the rules and principles of international law application to the states' cyber behavior in the context of ensuring global security. Meanwhile, the scientist notes the urgent need to define a common legal framework for the international law application in cyberspace. Eggett (2019) convinces that the systemic coherence of the international legal system elements with the system of general principles and norms becomes essential.

Adams & Reiss (2018), while surveying the specifics of harmonization of international and domestic law in cyberspace, found that unresolved and unsettled are the following issues: the problematic issues of social media exploitation in the gray zone; countering information war in cyberspace; timely detection of threats and risks. In addition, the authors argue that current international law applies to cyberspace but needs to be improved in terms of preventing cyber-attacks.

Kulesza & Weber (2021) and Nazarchuk (2019) convince that virtual space has a significant impact on the formation of international law, as many transactions of financial, economic, legal, and socio-political origin are carried out using it. Therefore, it is evident that international law is formed under the influence of cyberspace tendencies. At the same time, Fischerkeller (2021) categorically denies the application of international law to cyberspace. In particular, he means the UN Charter and customary international law justifying it by contradictions regarding terminological statements specified in such acts, while the strategic cyber environment is interpreted as the use of special codes by states to unilaterally inflict cyber vulnerabilities on other states, threatening their stability and strategic development. It is also proved by Maurer (2016), who argues that individual states use means to project power through cyberspace, thereby causing significant harm to other states. States, as cyberspace norms develop, will initiate the interpretation of current international law through the prism of promoting their national interests, deterring the unlawful behavior of other regional associations in shaping the international law system (Schmitt, 2020), which also is proved in the works by Alshdaifat (2017).

Undoubtedly, the problems of the international law impacts on cyberspace are under active consideration, as evidenced by the scientific heritage of Shelke & Gurpur (2021), who established a

close relationship between international law and national law regarding the regulation of legal relations arising in cyberspace. Likewise, Ülgül et al. (2020) associate the achievement of high-level global security and the formation of effective state and international organizations' security policy with the effectiveness of international law and its ability to prevent and timely counteract threats to cyberspace, which are recognized as one of the most critical problems of modern international relations. At the same time, Nirmal & Singh (2019) emphasize the changeability of current international law, which is easily influenced by destabilizing factors, challenges, and problems. Moreover, Odermatt (2021) proves the strong influence of the European Union law on it.

Adonis (2020), in complete agreement with previous researchers, has analyzed the current challenges of international law in the context of cyberspace governance and established the impact of digital sovereignty on it. The research results show that the effectiveness of the international law system in cyberspace functioning is ineffective in the countries affected by the global challenges of social and legal nature. At the same time, the lack of unification of international norms and their harmonization with the norms of national legislation is due to the diversity of scientific views on the jurisdiction, arbitration, and legal instruments to ensure the principles and characteristics of international law.

This study aims to substantiate the theoretical and applied research principles of current international law features and assess its impact on cyberspace.

3 Materials and methods

The study uses general scientific and special methods of economic analysis, namely: analysis and synthesis to determine the essence of current international law; analogy and comparison to carrying out analytical assessments of the current state and trends in the implementation of norms, principles, and organizational and legal foundations of current international law, as well as its impact on cyberspace; generalization and systematization in the formation of hypotheses, conclusions, and research results; grouping and cluster analysis based on the k-means method for grouping the European Union countries according to the Fragile States Index and the Global Cybersecurity Index (GSI); graphic and tabular ways to visualize the study results.

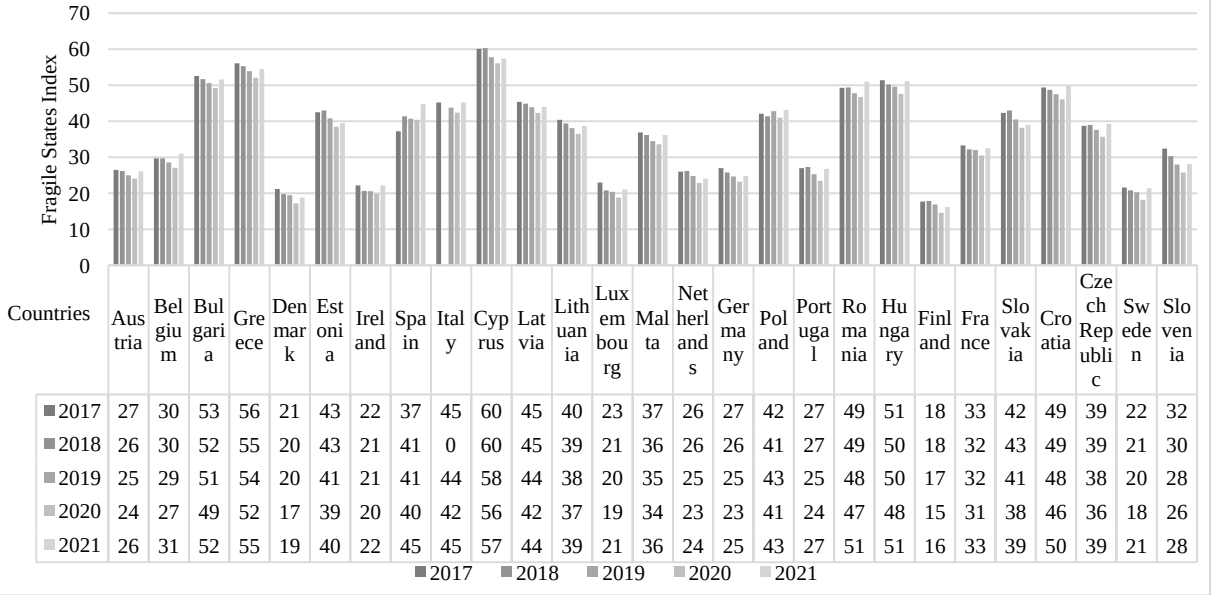
We chose the European Union countries for the study.

The information database of the study is based on reports from 2017 to 2021: List of Countries by Fragile States Index and Global Cybersecurity Index.

4 Results

Current international law functions as a separate organizational and legal system, combining a set of diverse elements that determine the international legal relations within the global community. The globalization and integration processes into regional associations, for example, the European Union, have entailed significant disruptive changes. The progressive influence on the national legal systems is assumed in this context. According to common development priorities, the countries' association reflects a higher level of consolidation of democracy, sovereignty, territorial integrity, and inviolability. The evidence of the countries' ability to ensure the outlined priorities is the calculation of the Fragile States Index. Its value has an inverse correlation with the stable functioning of the state. For example, when the Fragile States Index increases, the processes of socio-political and socio-economic instability are intensified. Figure 1 shows the tendencies of the Fragile States Index in the European Union in 2017-2021.

Figure 1: Dynamics of the Fragile States Index in the European Union in 2017-2021



Calculated according to the List of Countries by Fragile States Index, 2017–2020; Fragile States Index 2021

According to the calculations, Cyprus (FSI: 56-60), Greece (FSI: 52-56), and Bulgaria (FSI: 49-53) have the highest level of state fragility. On the other hand, Finland (FSI: 15-18), Denmark (FSI: 17-21), Sweden (FSI: 18-22), and Luxembourg (FSI: 19-23) are considered the most stable countries by the Fragility Index. One of the most important criteria for assessing the Fragile State Index is the effectiveness of a country's legal and regulatory framework and its implementation of the international legal norms. In this context, it is necessary to focus on Cyprus, which is one of the largest European offshore zones with the most significant number of registered offshore jurisdictions. Its legal framework is characterized by loyalty compared to international law norms, simplified tax legislation, attractive monetary and fiscal regime, simplified business registration procedure, high level of transactions secrecy, and enhanced protection of the banking sector.

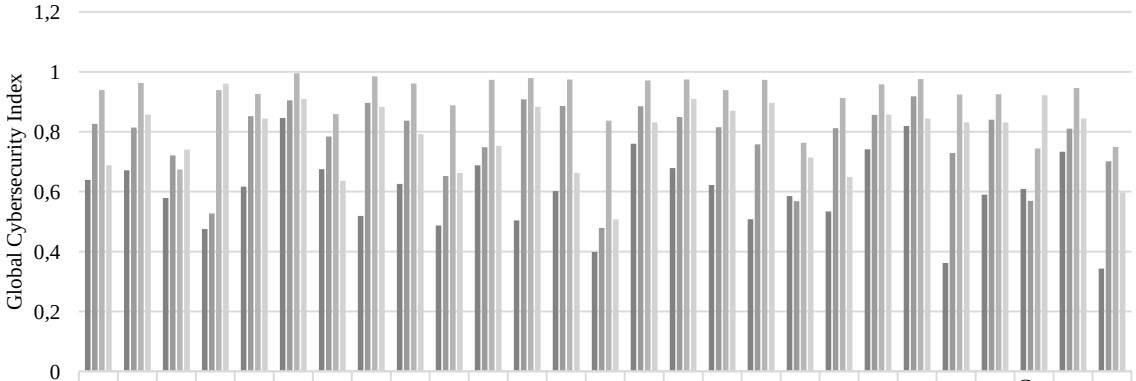
Nevertheless, today's realities indicate specific problems related to the legal protection of transactions in the virtual space. As a result, most European Union countries experience unauthorized interference and unlawful actions carried out through cyberspace. Such a situation leads to the need to develop a set of

measures to prevent and counteract risks and threats to cybersecurity. It, in turn, requires empirical assessments of the security level in this area. It has been proved that under globalization, it is hard to effectively counteract and prevent the challenges, dangers, and threats that arise in cyberspace and harm world countries' socio-economic and socio-political processes. Internationally, to measure the readiness of countries to prevent cyber threats and risks, it was formulated and proposed to calculate the Global Cybersecurity Index according to such essential criteria as:

1) ability to identify threats;
2) establishment of a security system;
3) development of cybersecurity education.

The current state and tendencies of the Global Cybersecurity Index in the European Union during 2017-2021 are shown in Figure 2.

Figure 2: Dynamics of the Global Cybersecurity Index in the European Union in 2017-2021.*



Countries	Austria	Belgium	Bulgaria	Greece	Denmark	Estonia	Ireland	Spain	Italy	Cyprus	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Germany	Poland	Portugal	Romania	Hungary	Finland	France	Slovakia	Croatia	Czech Republic	Sweden	Slovenia
2017	0,6	0,7	0,6	0,5	0,6	0,8	0,7	0,5	0,6	0,5	0,7	0,5	0,6	0,4	0,8	0,7	0,6	0,5	0,6	0,5	0,7	0,8	0,4	0,6	0,6	0,7	0,3
2018	0,8	0,8	0,7	0,5	0,9	0,9	0,8	0,9	0,8	0,7	0,7	0,9	0,9	0,5	0,9	0,8	0,8	0,8	0,6	0,8	0,9	0,9	0,7	0,8	0,6	0,8	0,7
2020	0,9	1	0,7	0,9	0,9	1	0,9	1	1	0,9	1	1	1	0,8	1	1	0,9	1	0,8	0,9	1	1	0,9	0,9	0,7	0,9	0,7
2021	0,7	0,9	0,7	1	0,8	0,9	0,6	0,9	0,8	0,7	0,8	0,9	0,7	0,5	0,8	0,9	0,9	0,9	0,7	0,6	0,9	0,8	0,8	0,8	0,9	0,8	0,6

*for 2019, there is no data on the Global Cybersecurity Index, as its value has not been calculated.
Calculated according to the Global Cybersecurity Index (GSI), 2017–2021

The research results of the Global Cybersecurity Index in the European Union in 2017-2021 allow us to state that there is no stable tendency for this indicator among the analyzed countries. The highest scores are recorded in such countries as France (GCI: 0,82-0,98), the Netherlands (GCI: 0,76-0,97), Finland (GCI: 0,74-0,96), and Sweden (GCI: 0,73-0,95), which indicates the effectiveness of the national system to counter the challenges, threats, and dangers in cyberspace. At the same time, the lowest scores are in Slovenia (GCI: 0,34-0,75), Slovakia (GCI: 0,36-0,92), Malta (GCI: 0,40-0,84), and Cyprus (GCI: 0,49-0,89), confirming the weakness and imperfection of the organizational and legal mechanism for countering cyber threats and risks.

To deepen empirical research, we consider it appropriate to group the European Union countries according to the Fragile States Index and the Global Cybersecurity Index within the analyzed timeframe to determine the standard and distinctive features of dealing with cybercrime, for which we use cluster analysis technology based on the k-means method (Table 1).

The results of the European Union countries clustering according to the Fragile States Index and the Global Cybersecurity Index in 2017-2021 allow us to identify three groups of countries characterized by standard features of state stability and risk resilience. The first group includes Austria, Belgium, Denmark, Finland, Ireland, Luxembourg, the Netherlands, Germany, Portugal, and Sweden. These countries are highly developed and have an adequate level of international law enforcement, effective response to cyber threats and risks, and close cooperation with other European Union countries in providing legal assistance to less developed countries. Therefore, ensuring national security in all its components and state stability is of great importance in such countries.

The second cluster includes Estonia, Spain, Lithuania, Malta, Poland, France, Slovakia, the Czech Republic, and Slovenia. They are characterized as countries with a medium level of development, but the legal framework is unstable, imperfect, and requires revision. In addition, some countries of this group went through a transformational stage of post-socialist reorganization (perestroika). It significantly impacted the formation of the legal framework and the harmonization of national legislation with the international law norms. In addition, Spain provides for simultaneous harmonization of national legislation with European and international ones through establishing supranational control over compliance with international normative and legal acts.

The third group includes Bulgaria, Greece, Italy, Cyprus, Latvia, Romania, Hungary, and Croatia, characterized as countries that have not completed the transformation processes, and ensuring state stability and cybersecurity is subject to the constant influence of destabilizing factors. Therefore, their counteraction depends significantly on the legal framework of international law and effective interaction with international organizations.

According to the studies conducted, it can be argued that there is no stable tendency for effective implementation of the principles and norms of current international law among the European Union countries. At the same time, we can state that globalization, mega-regionalization, and geopolitization create additional opportunities for developing the international law system, the particular actualization of which is observed in cyberspace.

5 Discussion

The research results on the features of current international law and the assessment of its impact on cyberspace allow us to identify three groups of European Union countries with typical features of ensuring the norms and principles of international law.

Group 1. Highly developed countries at a high level ensure the implementation of international law principles, compliance with its norms, and security guarantees in cyberspace. Also, they provide international legal assistance to developing countries (Austria, Belgium, Denmark, Finland, Ireland, Luxembourg, Netherlands, Germany, Portugal, and Sweden).

Table 1: Classification of European Union countries according to Fragile States Index and Global Cybersecurity Index in 2017-2021*

2017		2018		2020		2021	
Country	**Cluster number**	**Country**	**Cluster number**	**Country**	**Cluster number**	**Country**	**Cluster number**
Austria	1	Italy	1	Austria	1	Austria	1
Belgium		Austria	2	Belgium		Denmark	
Denmark		Belgium		Denmark		Ireland	
Ireland		Denmark		Ireland		Luxembourg	
Luxembourg		Ireland		Luxembourg		Netherlands	
Netherlands		Luxembourg		Netherlands		Germany	
Germany		Netherlands		Germany		Portugal	
Portugal		Germany		Portugal		Finland	
Finland		Portugal		Finland		Sweden	
Sweden		Finland		Sweden		Slovenia	
Estonia	2	France		Slovenia		Belgium	2
Spain		Sweden		Estonia	2	Estonia	
Lithuania		Slovenia		Spain		Latvia	
Malta		Bulgaria	3	Italy		Lithuania	
Poland		Greece		Latvia		Malta	
France		Estonia		Lithuania		Poland	
Slovakia		Spain		Malta		France	
Czech Republic		Cyprus		Poland		Slovakia	
Slovenia		Latvia		France		Czech Republic	
Bulgaria	3	Lithuania		Slovakia		Bulgaria	3
Greece		Malta		Czech Republic		Greece	
Italy		Poland		Bulgaria	3	Spain	
Cyprus		Romania		Greece		Italy	
Latvia		Hungary		Cyprus		Cyprus	
Romania		Slovakia		Romania		Romania	
Hungary		Croatia		Hungary		Hungary	
Croatia		Czech Republic		Croatia		Croatia	

*for 2019, there is no data on the Global Cybersecurity Index, as its value has not been calculated.
Calculated according to the List of Countries by Fragile States Index, 2017–2020; Fragile States Index 2021; Global Cybersecurity Index (GSI), 2017–2021

Group 2. Mid-developed countries ensure a sufficiently high level of introduction and implementation of international law. Still, some of them have not completed the process of implementation and unification of national legislation with international law, and the organizational mechanism of supranational control is unstable with elements typical for transition-type countries (Estonia, Spain, Lithuania, Malta, Poland, France, Slovakia, Czech Republic, and Slovenia).

Group 3. Developing countries are close to transition-type ones in terms of their development. Some of them have not yet completed structural reorganization. They need support and assistance in overcoming challenges, dangers, and threats from highly developed countries, while the normative and legal support of the international law implementation is not fully formed and requires revision (Bulgaria, Greece, Italy, Cyprus, Latvia, Romania, Hungary, and Croatia).

We should note that ensuring the norms of current international law cannot be limited to the European Union's borders but must consider the security standards of other countries within the framework of the transatlantic partnership since the functioning of cyberspace is transnational by its nature.

6 Conclusion

Thus, the conducted studies of the features of current international law and the assessment of its impact on cyberspace give reasons to conclude that it is a special legal system and the primary regulator of international relations. It ensures organizational and legal interaction mechanisms between countries and international organizations, particularly in cyberspace. We found that the intensification of virtual cyberspace development increases the risks of emergence and aggravation of the cyber threats' impact on national legal systems. That requires the implementation of national legislation with the norms of international law.

The most significant cyber threats at the present stage are recognized information warfare in cyberspace and exploitation of social media in the gray zone. Furthermore, it is proved that the decline of cyber security in the European Union entails an increase in state instability, most noticeable in Cyprus (FSI: 56-60; GCI: 0,49-0,89), which is one of the largest offshore zones with loyal fiscal legislation and low level of national legislation harmonization with international law norms.

Literature:

1. Adams, M.J. & Reiss, M. (2018). *International Law and Cyberspace: Evolving Views. Cybersecurity and Deterrence.* Available at: https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views
2. Adonis, A.A. (2020). *International Law on Cyber Security in the Age of Digital Sovereignty*. E–International Relations, 1–5. Available at: https://www.e-ir.info/pdf/82169
3. Al–Mahrouqi, A., Cianain, C.O. & Kechadi, T. (2015). *Cyberspace Challenges and Law Limitations*. International Journal of Advanced Computer Science and Applications, 6, 8. https://doi.org/10.14569/IJACSA.2015.060837
4. Alshdaifat, S.A. (2017). *A visible theme in the History of International Law: international or global*. International Journal

of Public Law and Policy, 6, 1, 54–77. https://doi.org/10.1504/IJPLAP.2017.085611
5. Bargiacchi, P. (2020). *Cyberspace and International Law*. International Workshop at Dokuz Eylul University, 12. Available at: https://www.academia.edu/44350226/CYBERSPACE_AND_INTERNATIONAL_LAW
6. Eggett, C. (2019). *The Role of Principles and General Principles in the Constitutional Processes of International Law*. Netherlands International Law Review, 66, 197–217. https://doi.org/10.1007/s40802-019-00139-1
7. Fischerkeller, M.P. (2021*). Current International Law is Not an Adequate Regime for Cyberspace*. LawFare, International Law. Available at: https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace
8. Fragile States Index 2021. Available at: https://fragilestatesindex.org/?msclkid=cbf4e627cf6b11ec88dc1f6cc4625338
9. Global Cybersecurity Index (GSI) 2017. Available at: https://www.cybersecobservatory.com/2017/07/07/global-cybersecurity-index-gci-2017/#
10. Global Cybersecurity Index (GSI) 2018. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
11. Global Cybersecurity Index (GSI) 2020. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
12. Global Cybersecurity Index (GSI) 2021. Available at: http://handle.itu.int/11.1002/pub/8191d342-en
13. Kulesza, J. & Weber, R.H. (2021*). Protecting the Internet with international Law*. Computer Law & Security Review, 40. https://doi.org/10.1016/j.clsr.2021.105531
14. List of Countries by Fragile States Index 2017. Available at: https://en.wikipedia.org/wiki/List_of_countries_by_Fragile_States_Index?msclkid=f2048e6acf6b11ecbae4784db641028d;
15. List of Countries by Fragile States Index 2018. Available at: https://en.wikipedia.org/wiki/List_of_countries_by_Fragile_States_Index?msclkid=f2048e6acf6b11ecbae4784db641028d;
16. List of Countries by Fragile States Index 2019. Available at: https://en.wikipedia.org/wiki/List_of_countries_by_Fragile_States_Index?msclkid=f2048e6acf6b11ecbae4784db641028d;
17. List of Countries by Fragile States Index 2020. Available at: https://en.wikipedia.org/wiki/List_of_countries_by_Fragile_States_Index?msclkid=f2048e6acf6b11ecbae4784db641028d;
18. Maurer, T. (2016). *«Proxies» and Cyberspace*. Journal of Conflict and Security Law, 21, 3, 383–403. https://doi.org/10.1093/jcsl/krw015
19. Moulin, T. (2020). *Reviving the Principle of Non–Intervention in Cyberspace: The Path Forward*. Journal of Conflict and Security Law, 25, 3, 423–447. Available at: https://doi.org/10.1093/jcsl/kraa011
20. Nazarchuk, O. (2019). *Strategy of protection of financial security of joint stock companies*. Administrative Law and Process, (2(21), 34-41. https://doi.org/10.17721/2227-796X.2018.2.04
21. Nirmal, B.C. & Singh, R.K. (2019). *Contemporary Issues in International Law*. Environment, International Trade, Information Technology and Legal Education. Available at: https://doi.org/10.1007/978-981-10-6277-3
22. Odermatt, J. (2021). *International Law and the European Union.* Cambridge University Pres. https://doi.org/10.1017/9781108895705
23. Schmitt, M.N. (2020). *Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace*. Texas National Security Review, 3, 3, 32–47. http://dx.doi.org/10.26153/tsw/10224
24. Shelke, A. & Gurpur, S. (2021*). Problem of Jurisdiction in Cyberspace and its Impact on International and Domestic Law*. SSRN, 12, 7. http://dx.doi.org/10.2139/ssrn.3500049
25. Ülgül, M., Çinar, Yu., Öztarsu, M.F., Vilić, V., Varpahovskis, E. & Erendor, M.E. (2020). *Contemporary Issues in International Relations.* Cambridge Scholars Publishing. Available at: https://www.researchgate.net/publication/340249638_Contemporary_Issues_in_ International_Relations
26. Valori, G.E. (2022). *Cyberspace and intelligence: Threats to intelligence, business and personal data will increase in 2022*. Modern Diplomacy. Available at: https://moderndiplomacy.eu/2022/03/01/cyberspace-and-intelligence-threats-to-intelligence-business-and-personal-data-will-increase-in-2022/
27. Vihul, L. (2018). *The Application of International Law in Cyberspace: State of Play*. United Nation, Office for Disarmament Affairs. Available at: https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

Primary Paper Section: A

Secondary Paper Section: AG