Ukraine's Information Security Policy: at the Crossroads between Russia and the West*

Serhii Fedoniuk, Nataliia Karpchuk, Bohdan Yuskiv**

Abstract

This is a study of the development of Ukraine's information policy within the dichotomy of two concepts of information (or cyber) security – those of Russia and the West. Ukraine may have chosen a policy of integration into Western security structures; however, for decades, it has been firmly connected to the traditions and approaches inherent in the Russian concept of information security. This phenomenon has been observed in the positions taken by researchers and lawmakers in the country and causes some ambiguity. Here, we present an assessment of the contradictory characteristics of Ukraine's information security policy and compare its Russian influence with its orientation to the West. We conclude that Ukraine is still balancing between these two spheres. Exposure to Russia's concept remains in academic circles, but the legal and normative sphere tends to follow the Western approach; and gradually, Ukraine's subjectivity in information security issues is developing at the international level.

Keywords: information security; cyber security; information policy; Ukraine; international cooperation

DOI: 10.5817/PC2023-3-184

1. Introduction

Ukraine set a course for integration into the EU and NATO in its Constitution. In 2022 it applied for EU membership and now declares its European identity in every possible way.

* This study was conducted within the framework of the Jean Monnet Module 'EU Strategic Communications: Counteraction to Destructive Influences' (No. 101047033 ERASMUS-JMO-2021-MODULE).
** Associate Professor at the Department of International Communications and Political Analysis, Faculty of International Relations, Lesya Ukrainka Volyn National University, Voli Ave., 13, 43025 Lutsk, Ukraine; e-mail Sergii.Fedoniuk@vnu.edu.ua. ORCID 0000-0003-2853-8905; Professor at the Department of International Communications and Political Analysis, Faculty of International Relations, Lesya Ukrainka Volyn National University, Voli Ave., 13, 43025 Lutsk, Ukraine; e-mail Natalia.karpchuk@vnu.edu.ua. ORCID 0000-0002-9998-9538; Professor at the Economics and Business Management Department, Rivne State University of Humanities, Plastova 31, Rivne, Ukraine; e-mail yuskivb@ukr.net. ORCID 0000-0001-7621-5954.

However, discussions about its Europeanisation and Westernisation continue; its commitment to a Western identity has been questioned for decades (Madsen, 2007; Minesashvili, 2022) and there is a noticeable 'split' in the orientation of Ukraine's domestic and foreign policies towards Russia and the West (Doroshko, 2017; Legvold, 2022). G. Virchick and J. Harris assess such a position as critical and even threatening for this state (Virchick & Harris, 2022).

Ukraine has started the formal process of gaining EU membership and, in practical terms, is approximating to NATO standards. This has increased the interest of observers in understanding specific areas of its policy, specifically related to security. In this study, we consider the nature of Ukraine's information security policy in compliance with Western and Russian approaches.

Information security is defined as 'the protection of information and systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability' (Nieles, Dempsey & Yan Pillitteri, 2017, p. 7). 'Information security is not a static process and requires continuous monitoring and management to protect the confidentiality, integrity and availability of information as well as to ensure that new vulnerabilities and evolving threats are quickly identified and responded to accordingly' (Nieles et al., 2017, p. 10). To achieve this requires a specific policy – information security policy – which is an 'aggregate of directives, regulations, rules and practices that prescribe how an organisation [or a state – authors' note] manages, protects and distributes information' (NIST, 2022).

Two concepts of information security policy are used to understand the approach to information space in different socio-political systems. The first, developed in democratic countries (the West), is based on freedom of information, the independence of cyberspace (the state provides only technical regulation) and the absence of any ideological component (Christou, 2014; Taylor & Hoffmann, 2019). In the second concept, adopted by predominantly authoritarian states including Russia (Sharikov, 2018) and China (Gao, 2022), the state has a monopoly on the management of the information space including all the information it considers necessary to implement its power priorities.

Since its independence in 1991, Ukraine has remained under the powerful influence of Russia in all spheres of life, and the formal announcement of a course to Euro-integration in early 2000 did not bring any significant changes. The turning point was in 2014 when Russia began military aggression against Ukraine. This created the impetus for further orientation towards Europe, European values and the West.

In this article we present an analysis of the influence of the two approaches to information security – those of Russia and the West – on Ukraine's academic and legal framework.

The empirical sources of our research include scientific publications, current and draft legislation, and evidence of international cooperation by Ukraine in the field of information security. The time frame covers the period from 1991 to 2022. Having found no objective material in the literature on Ukraine's international cooperation on information security policy, which is often reported with bias by researchers, we have analysed the topic comprehensively.

Our research methodology was to analyse the sources descriptively, make a comparative examination of information security policy, related issues and challenges, and

conduct a qualitative study of Ukraine's actions and published statements in domestic and foreign policy.

The article is structured as follows. The introduction outlines the aim and the frame of the research. The second section provides background on the dichotomy of the Western and Russian approaches to information security issues, particularly the growing divergence in their attitudes. The third section draws on the academic and normative influence of Russia on Ukraine's information security. The fourth section is an analysis of Ukraine's efforts to follow and comply with Western standards and principles regarding information security policy. The article concludes with an evaluation of our analysis.

2. The dichotomy of approaches to information security issues

The differences between the Western and Russian concepts are manifested in various aspects of information security policy, particularly in combating cyber crime, preventing terrorism and countering threats of a military-political nature, as well as in the application of international law and international cooperation on cyber security. For almost two decades, Russia has opposed the establishment of one international standard for combating cyber crime, i.e., the Council of Europe's Convention on Cybercrime, known as the Budapest Convention (Council of Europe, 2001), while promoting an alternative document at the UN level, i.e., the Draft United Nations Convention on Cooperation in the Field of Combating Information Crime (United Nations, 2017). Russia does not accept the Budapest Convention's article on 'cross-border access to stored computer data', which would allow various intelligence services to conduct operations on third-country computer networks without official notification, claiming it threatens the country's security and sovereignty. Russia's perception of cyber terrorism is also different from that of the West, where this is seen as a threat to information systems, primarily critical infrastructure (Janczewski & Colarik, 2008, p. 13), whereas, in Russia, cyber terrorism is taken to include complex threats to the individual, society and the state (Ivanov & Tomilov, 2013) (the Chinese government also follows this approach).

The approaches to information security in terms of military-political strategy contradict as well. Authoritarian systems use the idea of integrated influence of the power structures and the state-controlled media sector, i.e., the concept of 'information warfare' (Turonok, 2003; Panarin, 2006; Anichkina, 2007). Instead, democracies (primarily the United States and other NATO members) support media independence and separate military and civilian information influences on the realisation of the government's strategic interests, i.e., the concept of 'strategic communications' (NATO, 2009). Western countries are characterised by a purely utilitarian idea of using cyberspace in a military-political context (Szafranski, 1995; Molander, Riddlie & Wilson, 1996; Libicki, 2009). They consider the concept of 'information warfare' closer to the actual context, although often in a multidisciplinary sense (Ivančík, 2021).

These different concepts of information security result in fundamentally different approaches to applying international law in this area. Western countries perceive cyberspace as a continuation of 'normal' relations in society, particularly regarding information security. Thus, the National Cyber Strategy of the United States of America, 2018, reflects an in-depth approach to assessing the risks associated with cyberspace and integrates cyber activities into the system of power relations. 'Cyberspace will no longer be considered a category of policy or activities separate from other elements of national power. The United States will integrate the use of cyber options into all elements of national power' (the White House, 2018). From a legal point of view, the position of NATO members on information security is presented in the Tallinn Manual (Schmitt, 2013; Schmitt, 2017), which convincingly demonstrates the relevance of applying existing international law to cyberspace. The exact position is typical for Western countries (Greenberg, Goodman & Soo Hoo, 1997).

However, Russian authors insist on adapting the law to the specifics of the information space (Krutskih, 2007; Korotkov & Zinovieva, 2011; Fedorov & Zinovieva, 2017). Russia's concept of the legal regime and format of cooperation in this area, known as 'international information security' is also supported by other states with a low level of democracy including China, which advocates special mandatory 'rules of conduct'. Since the late 1990s, on the main international platforms, Russia has been promoting draft decisions on the leading role of the state in all processes of informatisation, telecommunications and internet governance (Akushev, 1999; Bykov, 2008), the issue of 'information sovereignty' (United Nations, 1999; United Nations, 2018b), drafts on 'rules of conduct' in cyberspace and conventions on cyber crime (United Nations, 2015).

Russian initiatives are generally supported by China, which insists on cyber sovereignty (Hao, 2017) and offers an authoritarian model of internet governance (the Wuzhen Initiatives) (Zhu, 2015). This runs counter to the well-established model of global network management Western countries seek to preserve. The US stands for a liberal approach to developing cyberspace and multilateral internet governance (MacLean, 2005; Hofmann, 2007; Kurbalija, 2014; Balzacq & Cavelty, 2016). It advocates the concept of optional norms of behaviour in cyberspace and has suggested a draft UN resolution: Encouraging the responsible behaviour of states in cyberspace in the context of international security 2018 (United Nations, 2018a).

The interpretation of the concept of 'information security' in Russia creates a dichotomy with the West and is similar to that in other authoritarian countries. Such states include political and ideological aspects in the meaning of 'information security,' namely: countering propaganda, preventing destructive information influence and interference, ensuring the security of information. Information is declared an integral component of national sovereignty. Scholars (primarily Russian) consider four main threats to national and international security in the information sphere: crime threats, terrorism, military and political influence, and public disorder and instability by impact on the state's public opinion (Shvets, 2005; Smirnov, 2011; Kucheryavyi, 2013).

Instead, in states with freedom of information, computer networks and resources are protected (information is secure as long as the relevant infrastructure is secure). This is treated as 'cyber security', and governments provide their citizens with the freedom and

security to use information and communication technologies. This approach is also applied to developing regulatory frameworks for cyber security in the international arena (Finnemore, 2011; Farrell, 2015). In academic discourse, threats to cyberspace of a criminal, terrorist or military-political nature are considered mainly in the context of their information or technical impact (Wenger, 2001; Hansen & Nissenbaum, 2009; Giacomello, 2016; Tikk-Ringas, 2015).

International cooperation in information security takes place on various platforms; mainly negotiating tracks at the UN, e.g., within the UN Group of Governmental Experts (UN GGE) and, more recently, the Open-ended Working Group (OEWG), which is the result of strategic competition between the United States and Russia. The UN GGE has developed approaches close to the US position, while the OEWG track is for the development of cooperation at the UN level on the initiative of Russia (Schmitt, 2021).

The European Union has joined the dualistic system of counterbalances in information security formed over the recent years at the UN. Since 2020, the EU has become increasingly active and has adopted its own strategy (European Commission, 2020). The EU also proposed a novel format for the interaction of parties at the UN, aimed at promoting responsible behaviour of states in cyberspace, which generally reflects the Western concept (United Nations, 2020). In light of the long-standing competition between Russia/China and Western approaches to information security, this was seen as an attempt to bridge the dichotomy of cyber issues at the UN within the UN GGE and OEWG.

3. Russia's impact on the academic and legal vision of Ukraine's information security policy

Since the 1990s and throughout the years of Ukraine's independence, its information security has been oriented towards the Russian concept, both in the legal approach and scientific research. This is explained by the common origin of the information space and the continuity of professional experience in law and science dating back to Soviet times. One of the leading indicators is the emphasis on 'information sovereignty', that is, the exclusive power of the state to dispose of 'information resources belonging to it'. Such information sovereignty is mentioned in the Law of Ukraine on Information (Verkhovna Rada of Ukraine, 1992), amended in 2011, in the Law of Ukraine on the National Informatisation Programme (Verkhovna Rada of Ukraine, 1998) and in some other legal documents. The 2009 Doctrine of Information Security of Ukraine states that one of its main goals is 'to create a developed national information space in Ukraine and protect its information sovereignty' (Verkhovna Rada of Ukraine, 2009).

At the end of the 1990s, a concept of information policy was developed based on 'information sovereignty' and 'national information space', which was reflected in the above-mentioned Russian initiatives at the UN level. In Ukraine in 1998, a draft Law on Information Sovereignty and Information Security of Ukraine defined 'information sovereignty' as 'the right of the state to form and implement national information policy under the Constitution and legislation of Ukraine, and under international law in the

national information space of Ukraine' (Verkhovna Rada of Ukraine, 1998a). Another bill appearing in 1999 (Verkhovna Rada of Ukraine, 1999) focused similarly on information sovereignty. The 1998 Law of Ukraine on the National Informatisation Programme defined 'information sovereignty' as 'the ability of the state to control and regulate the flow of information from outside the state to comply with Ukrainian laws, rights and freedoms, and guarantee national security' (Verkhovna Rada of Ukraine, 1998b).

In the late 2000s the internet posed new challenges, and a new wave of interest in 'information sovereignty' appeared. Notably, the Draft Law on the Concept of State Information Policy, 2010 claimed that the need to 'ensure effective protection of Ukraine's information sovereignty, especially the domestic segment of the internet' was an essential task of state security (Verkhovna Rada of Ukraine, 2010). In essence, the legislators meant to achieve what had already been done in China and Russia: to single out and protect the 'sovereign internet'. At the same time, the concept of state policy on information sovereignty (analytical report of the National Institute for Strategic Studies) (NISD, 2014) was offered. However, the wording 'information sovereignty' and an article were removed from the Law of Ukraine on Information, 2011 as it 'does not belong to the principles applied in at least one human rights treaty'. The amendment was made after considering the recommendations of Council of Europe experts (UHHRU, 2007).

The interpretation in Ukrainian legislation of such notions as 'national information space', 'information relations', 'information security' and the concept of the state as the 'owner' of information is typical of authoritarian states. For example, the idea of 'national information space' was not entirely compatible with Article 19 of the International Covenant on Civil and Political Rights (United Nations, 1976) in which the right to freedom of speech and right to information exist without regard to national borders. The owner of the information is not any public authority that disposes of it, but taxpayers (the public) due to whom the information has been created and is being processed.

Concerning 'information security', expert opinion claims that information at the disposal of the state is public property, and it can be removed from this category if its distribution could harm the interests that the state can protect on legal grounds (particularly, the interests of national security, which require the storage of certain information so that only a few representatives of the government or the military can access it). Such restrictions are necessary, must meet the criterion of public interest (for example, during martial law) and are always temporary (UHHRU, 2007).

Today, the concept of 'information security' is formalised in Ukrainian law, which generally corresponds to the well-defined concept of protection of national security interests in international law, i.e., protection against attack, the overthrow of the constitutional order etc., particularly, protection of Ukrainian society from aggressive information influence to propagate war, incitement of national and religious enmity, change of the constitutional order by violent means or violation of the sovereignty and territorial integrity of Ukraine (President of Ukraine, 2017).

Because of the Russian military aggression, which started in 2014, the issue of information security has become especially relevant as the information sphere turned into a battle field. On this basis, there are proposals to develop a fundamental law (information code), which will include a separate section on information security, or to adopt a particular Law

of Ukraine on the Information Security of Ukraine, which 'will be able to regulate the state policy basic principles aimed at protecting the information security of people, society and the state from external and internal threats' (Shevchuk, 2021, p. 213).

In academic circles, there is a widespread opinion about the state's exclusive role in information circulation. This position influences the development of such concepts as 'national information space' and 'information sovereignty'. It represents the authoritarian model typical of Russia's 'information security' concept: 'the function of the state as the main subject of information sovereignty is not limited to controlling information flows, but also involves the state's informational influence on its citizens to ensure the national interests of the state in the information field' (Solodka, 2020a).

While singling out cyber security, some authors still support a strong position for the state in information security and the information space (Horlynskyi & Horlynskyi, 2019). Other researchers suggest strictly regulating access to mass information to 'protect the citizens of Ukraine from destructive (information) influence' (Averianova & Voropayeva, 2020). The issue of 'information sovereignty' has re-emerged in scientific discourse and is treated as 'a legal feature of the supremacy, independence, completeness and indivisibility of its power in the information space of Ukraine' (Solodka, 2020b, p. 237). Modern publications focus on the 'sovereignisation' of the information space, which is typical of authoritarian states: 'normative and legal regulation of the formation of Ukraine's unified information space should contribute to the harmonious development of information resources, information services and information products in the country' (Havryltsiv, 2020, p. 203).

On the threshold of the third decade of the 21st century, attempts to regulate access to information do not stop, motivated by concern for national security. In 2019, the Ministry of Culture, Youth and Sports of Ukraine introduced a draft Law on Amendments to Certain Legislative Acts of Ukraine on Ensuring National Information Security and the Right to Access Reliable Information. This offered to strengthen the concept of protecting the 'national information space' from unwanted information under the guise of combating disinformation (MCIPU, 2020). Even recent studies reserve for the state a certain exclusive role in the issue of subjectivity in 'information relations'. They define 'information security' as 'a certain state of security of the information environment of Ukrainian society, due to which such society is developed as an information subject (including individuals, groups and the state as an information subject)' (Sopilko, 2021, p. 20).

Some Ukrainian scholars are in favour of the concept formulated in the Russian-initiated resolutions Achievements in Information and Telecommunications in the Context of International Security, as they do not consider other documents and initiatives. For example, V. Nastyuk and V. Bielievtseva argue that 'information security includes issues such as confronting cultural expansion by countries with developed audiovisual industries, preserving national and linguistic identity' (Nastyuk & Bielievtseva, 2014, p. 42). They share views on the development of international law in the field of information security, which is characteristic of Russia and its satellites: 'it is necessary to develop international principles (regime, code of conduct of states) aimed at strengthening international information security, which initially could be made in the form of a multilateral declaration,

and, in the future, fixed in the form of a multilateral international legal document' (Nastyuk & Bielievtseva, 2014, p. 42).

O. Frolova praises the role of the UN in the 'system of international information security', and positively assesses the initiatives of the state-dominated concept followers in matters of freedom of information, particularly in the context of the 'regime of international information security' (Frolova, 2018). This is consistent with Russian strategy in this area (MFARF, 2011; Security Council of the Russian Federation, 2021). She seems to favour the Russian draft UN General Assembly resolution 73/27 Achievements in the field of information and telecommunications in the context of international security, 2018 and considers this a positive shift in regulatory and organisational support (Frolova, 2019, p. 125). Resolution 73/768 Encouraging responsible behaviour of states in cyberspace in the context of international security, adopted in parallel at the same session and initiated by the United States, is not mentioned by the researcher.

O. Kisilevych-Chornoivan (2009) substantiates building a separate 'information and security' domain in international law and the formation of 'international information security', referring to the above-mentioned Russian-initiated resolutions of the UN General Assembly (Kisilevych-Chornoivan, 2009). A. Voitsikhovskyi (2020) promotes the same idea: 'one of the areas of international activities in the information field is the formation and improvement of a system of international information security' (Voitsikhovskiy, 2020, p. 284). However, the author does not mention the initiatives of democratic countries. A. Kostyrev explains the contradictions between the West and Russia in their approaches to information security by their commitment to idealistic and realistic paradigms. Nevertheless, he insists on the need for the active participation of the state in the development of norms of international information law, their implementation and control over the implementation by all subjects of information relations (Kostyrev, 2010).

At the same time, the balanced position of foreign policy practitioners is worth mentioning. Thus, Yu. Romanchuk, an expert diplomat and scientist, draws attention to the need to find a solution for Ukraine to the problem of disagreements in the leading global approaches to information security policy. He supports the prospect of the 'codification of special principles and norms based on the UN Charter and the achievement of new agreements to regulate and stabilise the relations of states concerning the problem of information security. 'The diplomat emphasises that Ukraine is interested in overcoming the destructive dichotomy in managing global security policy in the context of conflicts between the interests of the United States and Russia' (Romanchuk, 2009). This indicates the complexity of information security in Ukraine. Recent publications by leading scientists in the field examine the real state of affairs in balancing the approaches of the main actors, countries and international organisations to information security policy (Kopiika, 2020).

The problem of information security in the international dimension is the subject of thorough studies in Ukraine, particularly in education where these issues are less dependent on specific political or state-strategic trends and approaches. For instance, the textbook International Information Security: Theory and Practice (Makarenko et al., 2016) reveals the security aspects of the strategies of international organisations, intergovernmental associations and individual states, although the title of the book is somewhat consistent

with the Russian concept of the international legal regime of 'international information security'.

4. The Western vector of Ukraine's information security policy

Ukraine's strategic course, as enshrined in the Constitution, to acquire full membership of the EU and NATO determines practical steps in foreign and domestic policy, as in strategic planning. A particular shift is indicated in the Cybersecurity Strategy of Ukraine, 'Safe cyberspace – the key to the successful development of Ukraine', adopted in August 2021. This replaced Ukraine's previous Cybersecurity Strategy, approved in March 2016 (President of Ukraine, 2016). Even then, the 2016 Strategy outlined primary directions characteristic of democracies, namely, the development of a national cyber security system with respect for human and civil rights and freedoms; ensuring national interests; open, accessible, sustainable and secure cyberspace; capacity building in the security and defence sector (cooperation with the private sector, civil society and the international community, adequate risk-based cyber security measures, priority of preventive measures); and establishing democratic civilian control in the field of cyber security.

Regarding international cooperation, the 2021 Strategy focuses on several priorities that may indicate compliance with Western countries' approach and a focus on collaboration with partners in the EU and NATO. It outlines the following (Verkhovna Rada of Ukraine, 2021): ensuring Ukraine's participation in UN activities to promote responsible behaviour of states in cyberspace; consistent support for the provisions of the Budapest Convention of the Council of Europe on Cybercrime; and strengthening cooperation with leading IT companies, global digital service providers and social networks.

The 2021 Strategy foreign policy priorities stipulate (Verkhovna Rada of Ukraine, 2021): unification of approaches, methods and means of cyber security with the established practices of the EU and NATO; mutually beneficial exchanges of information and experience with partner intelligence services of EU and NATO member states; lasting active participation in the international dialogue on responsible behaviour of states in cyberspace in compliance with the principles of international law, the UN Charter, as well as norms, rules and regulations of responsible behaviour of the state; maximum support for a multi-stakeholder (multilateral) model of internet governance involving representatives of the private sector, scientific and educational circles, civil society institutions (it is emphasised that the attempts of individual authoritarian states to sovereignise the internet contradict the long-term interests of Ukraine and its model of socio-economic development); and the promotion of further compliance with international human rights law and standards (Ukraine proposes that the internet should remain global and open, technologies should focus on people and their fundamental freedoms, guarantee non-interference in their personal lives, ensure their privacy in cyberspace, and any restrictions should be implemented only in accordance with the law).

The listed priorities fully correspond to the democratic Western concept of information security, in which the state's monopoly on internet governance is absent, human rights and freedoms are respected and states and stakeholders cooperate in a joint fight against cyber threats. The following assurance confirms this: 'Ukraine will cooperate with international partners, organisations and other interested parties that share our common vision of the future of cyberspace as global, open, free, stable and safe, based on the observance of human rights, fundamental freedoms and democratic values, which is key to the socio-economic and political development of Ukraine' (Verkhovna Rada of Ukraine, 2021). The strategy has been positively assessed by Ukrainian researchers as it 'will strengthen the national security of our state, as well as provide guarantees of human and citizen rights and freedoms in a democratic state' (Pravdiuk, 2022, p. 47).

At the same time, there is 'neutrality', or even uncertainty on some issues regarding the positioning of Ukraine's cyber security strategy within the dominant world policy concepts in this area. We compared the approved text of the Strategy with its draft (NSDC, 2021), published on Ukraine's National Security and Defence Council website, and found some discrepancies. There is a significant deviation from the specifics of formulating individual theses, which may indicate an attempt to avoid irrelevant positions in the future, given the long-term perspective of the document. For instance, the draft Strategy declares 'deepening European integration processes by unifying approaches, methods and means of ensuring cyber security with the established practices of the EU and NATO' to be 'the top foreign policy priority of Ukraine in the field of cyber security'. However, the final document does not mention this 'top priority'. The draft contains wording that is in line with the consensus adopted in 2015 by the UN GGE report on 'voluntary, non-binding norms, rules and principles of responsible state conduct', apparently referring to 11 norms, rules and principles published in this report (UN General Assembly, 2015). Instead, the document that came into force references compliance with certain 'norms, rules and principles of responsible conduct of the state' (without specification). The final text of the Strategy does not include an indication that Ukraine is supposed to participate in the work of the international platform of the Programme of Actions for Encouraging Responsible Behaviour of States in Cyberspace of the UN General Assembly and the UN Group of Governmental Experts on Information Security (UN GGE). This provision is replaced by a general wording on participation in 'international events of the UN on encouraging responsible behaviour of states in cyberspace'.

Ukraine did not participate in the UN GGE at the expert level (Digwatch, 2021). However, it did express its views on the UN secretary-general's annual report on changes in information and telecommunications in the context of international security (UNIDIR, 2021). There is also no information on the statement of Ukraine's position in the preparation of the OEWG report (UNODA, 2021). Instead, the official Facebook page of the Permanent Mission of Ukraine to the UN states that one of Ukraine's priorities in the activities of the Working Group includes the acquaintance of the international community with the state's position on issues within its competence. It is also mentioned that there is a need to launch the Programme of Action on Responsible Behaviour in Cyberspace of a group of countries (co-authored by 53 countries, including Ukraine). This means creating a single body to replace the previous two negotiating

platforms on cyber security and focus not only on drawing conclusions and recommendations but also on monitoring the implementation of decisions (Perm Mission of Ukraine, 2021b).

Thus, Ukraine co-authors the Programme of Action on Responsible Behaviour in Cyberspace. Specifically, Ukraine's Permanent Mission to the United Nations confirmed the application of international law in cyberspace, including the UN Charter, emphasised the importance of this Programme of Action and called for further substantive discussion of this initiative in future formats under the auspices of the UN. This should lead to a permanent institutional dialogue to 'terminate the existence of certain ICT working bodies in the context of international security' (Perm Mission of Ukraine, 2021a). Therefore, we can assume that Ukraine has chosen a Western approach to implementing an information security policy, which is followed by an increasing number of countries that support the Programme of Action.

In the context of coordinating positions with other democracies, Ukraine's cooperation in cyber security is strengthening with the European Union and the United States. In June 2021, the Ukraine-European Union Cyber Dialogue was launched. This is likely to have a goal similar to the EU-US cyber dialogue launched in 2014, namely to coordinate foreign policy on cyber issues, cooperate in strategic aspects of cyber security and discuss practical issues of cooperation in this area. The Ministry of Foreign Affairs of Ukraine claims by starting cooperation within the Cyber Dialogue, Ukraine and the EU will coordinate cooperation within international organisations to strengthen cyber resilience and ensure responsible behaviour in cyberspace. Ukraine's position aligns with the European vision of the Western concept of information security with strict adherence to the principles of democracy in the development of cyberspace. 'Ukraine and the EU reaffirmed their commitment to a global, open, stable and secure cyberspace that fully complies with the principles of the rule of law, in which the rights of individuals are equally protected online and offline, and in which the security, economic development, prosperity and unity of free and democratic societies are encouraged and properly protected' (MFA of Ukraine, 2021).

In terms of policy coordination, Ukraine confirms the importance of the Budapest Convention, which serves as a basis for national legislation and international cooperation to combat cyber crime. During the first meeting of the Cyber Dialogue, Ukraine presented its work on including the provisions of the Budapest Convention in national legislation, namely the draft laws amending the Criminal Procedure Code of Ukraine and the Code of Administrative Offences already approved by the relevant Verkhovna Rada Committee. With the European Union, Ukraine has committed to the swift adoption of the Second Additional Protocol draft to strengthen cooperation in cyber crime and electronic evidence and reaffirmed its continued support for international cooperation to combat cyber crime effectively in regional and international forums (EU4Digital, 2021; MFAU, 2021).

Table 1 presents the impact of the Russian and Western approaches on the development of information security policy in Ukraine.

Table 1: Western and Russian influences on Ukraine's information security policy			
Criteria	**Russia**	**Western states**	**Ukraine**
State control of information	full	absent	partial
Dominant understanding of security regarding advances in information and telecommunications	'information security'	'cyber security'	both
'Information sovereignty'	supported	rejected	discussed in academic research
Understanding of information space	national information space	global information space	national information space
Legal regime of 'international information security'	supported	rejected	not officially supported, but present in scientific discourse
Proposal of a special law on information security and development of 'rules of conduct' of states	supported; special 'rules of conduct' of states	rejected; voluntary 'rules of conduct' of states	rejected; voluntary 'rules of conduct' of states
Objects of information threats	person, society, state	information systems	person, society, state, but in the context of exclusively negative information influence of Russia
International cooperation to combat cyber crime based on the Budapest Convention	not supported	supported	supported
Understanding of 'cyber terrorism'	a threat to the person, society, state	utilitarian interpretation (as a threat to infrastructure, targeting non-combatants)	terrorist activity carried out in cyberspace or with its use (regarded also as a threat to the national security of the state in the context of Russia's armed aggression)
Understanding information threats of a military and political nature	integral understanding – the concept of 'information warfare'	differentiated understanding – the concept of 'strategic communications'	the concept of 'information warfare' is being replaced by the concept of 'strategic communications'
Internet governance	state	multistakeholder	multistakeholder
Source: The authors.			

The presence/absence of relevant norms in regulatory acts or other documents of significant importance in the internal or external policy of countries constitutes the grounds for the selected criteria:

– 'full' – there are relevant norms in national strategic planning documents (doctrines, strategies), directive legislation (laws, by-laws) and acts of international law adopted or promoted by the country;
– 'absent' – absence of the corresponding norms in national legislation, strategic planning documents and international acts adopted or promoted by the state;
– 'partial' – in the national legislation there are disagreements regarding a certain norm as a result of temporary restrictions or its ongoing change;

– 'supported' – in the national legislation there are norms to support a concept or a norm existing in world practice;
– 'not supported' – there is a lack of data on state support of a norm or concept existing in world practice;
– 'rejected' – either in the national legislation or in international acts adopted by the state or in its officially expressed positions there is a denial of the concept or norm existing in world practice.

For instance, in Russia, full state control of information is reflected in the 2019 laws on 'the sovereign internet' (Federal Law of 1 May 2019 N 90-FZ On Amending the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection' (Rossiyskaya Gazeta, 2019), which require internet providers to install special equipment to monitor, filter and redirect internet traffic, enabling Roskomnadzor to independently and extra-judicially block access to content the government deems threatening. Instead, the US information security democratic model is based on the Freedom of Information Act (FOIA, 2016) which enshrines the accountability of government to the people it serves, since an informed electorate is critical to the proper functioning of a democracy. Therefore, information security aims to ensure, on the one hand, the functioning of information systems for the proper activity of the executive power and its reporting to the people, and, on the other hand, the inviolability of information that belongs to a person in the same way as any other private property. The Privacy Act (US Department of Justice, 2022) establishes a code of fair information practices governing the collection, maintenance, use and distribution of personal information about individuals maintained in federal records systems. Also in the USA, freedom of expression and freedom of speech are guaranteed by the first amendment to the Constitution. In Ukraine, the right to freedom of information is guaranteed in Part 2 of Article 34 of the Constitution of Ukraine (Verkhovna Rada of Ukraine, 1996), but today there are temporary measures of information control during martial law due to the Russian military invasion.

Russian laws on 'the sovereign internet' mentioned above also determine the state management of the internet; the Federal Service of Supervision in the field of communications, information technologies and mass communications carries out the functions of control and supervision. By contrast, the Western model of multi-stakeholder internet management is implemented in the USA by the National Cyber Strategy (The White House, 2018) and in the EU by the Cybersecurity Strategy for the Digital Decade (European Commission, 2020). In Ukraine, this vision is present in foreign policy documents that support the Western approach. In particular, this is the official position of Ukraine agreed with civil society organisations at the 54th Conference of the Internet Corporation for Assigned Names and Numbers (ICANN), a second round of consultations on the review of the World Summit on the Information Society (WSIS+10), 2015, the 10th World Forum on Internet Governance (2015) and the WSIS+10 review process in the framework of the GA UN (European Media Platform, 2015).

In Russia, the information security concept is based on the Draft Convention on International Information Security (MFARF, 2011) and the Russian vision for a Convention of the UN on Ensuring International Information Security (UNODA, 2023), Fundamentals

of the state policy of the Russian Federation in the field of international information security (Decree of the President of the Russian Federation, 2021). These acts establish the regime of 'international information security' which defines Russian foreign policy in the security context. The EU's security position is fully disclosed in its Cybersecurity Strategy for the Digital Decade (European Commission, 2020). In Ukraine, the pro-Western position is outlined in the Cyber Security Strategy (Verkhovna Rada of Ukraine, 2021) and the Law on Cyber Security (Verkhovna Rada of Ukraine, 2017).

The USA does not support the Russian concept of 'international information security', as stated in Resolution 73/266 Advancing responsible state behaviour in cyberspace in the context of international security (United Nations, 2018a) and other similar acts. The US also carried out work in the UN GGE referred to above. This confrontation between the US and Russia continues (Weber, 2023).

Regarding 'information sovereignty', Russia's clear and unambiguous position is reflected in the above-mentioned acts on the 'sovereign internet' and the resolutions it offered on Developments in the field of information and telecommunications in the context of international security (United Nations 1999; United Nations 2018). This approach does not exist in the legislation of Western democratic states; it does not belong to the principles applied in human rights treaties. In Ukraine, the norm on information sovereignty was removed from the old version of the Law on Information back in 2011, but it is still being discussed among lawmakers and researchers.

The Russian idea of a national information space is based on the norms of the UN General Assembly on Developments in the field of information and telecommunications in the context of international security (United Nations 1999; United Nations 2018), while the Western perception of information space as single and universal, not divided between countries, is based on the UN International Covenant on Civil and Political Rights (United Nations, 1967). In Ukraine, the idea to single out a certain national cluster of the information space has long prevailed and has become more vital in the security context in wartime. Ukraine's Cyber Security Strategy (Verkhovna Rada of Ukraine, 2021) is its confirmation.

Russia persistently promotes the idea of creating a special domain of international information security law and developing 'rules of conduct' for states, in particular, through the above-mentioned resolutions. Western states are guided by the Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt, 2013), UN Resolution 73/266 Advancing responsible state behaviour in cyberspace in the context of international security (United Nations, 2018a) and other similar acts. Ukraine supports the Western stance. In 2021, there was an attempt to 'reconcile' the Russian and US positions when Resolution 76/19 (United Nations, 2021) combined the opposing visions, but the real 'reconciliation' is still a long way off.

The objects of information threats are clearly defined in official and regulatory documents: the Doctrine of Information Security of the Russian Federation (Rossiyskaya Gazeta, 2016), the ENISA Threat Landscape Report (ENISA, 2022) and Ukraine's Information Security Strategy (President of Ukraine, 2021).

Understanding cyber terrorism is a bit more complicated. Its Russian interpretation as a threat to 'the person, society and the state', widespread in the scientific literature, is not

reflected in the legislation, and a purely utilitarian and specific interpretation is also found in US departmental documents – e.g., Terrorism Report 2002–2005 (US Department of Justice, 2015). In Ukraine, it is also not defined normatively, but the concept is mentioned in the national Cyber Security Strategy (Verkhovna Rada of Ukraine, 2021) in a context as close as possible to the American treatment.

The Russian understanding of threats of a military and political nature is normatively reflected in the Military Doctrine of the Russian Federation (Rossiyskaya Gazeta, 2014) and the strategic planning document of the Russian Ministry of Defence – Conceptual views on the activities of the armed forces of the Russian Federation in the information space (Ministry of Defence, 2011). Regarding Western countries' approach, the final design of the strategic communications system is fixed in the March 2023 NATO standard – Allied Joint Doctrine for Strategic Communications (NATO, 2023), which also summarises previously adopted acts. In Ukraine, similar documents have been adopted by the Ministry of Defence and the Information Security Strategy defined the corresponding directions of strategic communications development (President of Ukraine, 2021).

5. Conclusion

For a long time, Ukraine has not shown subjectivity in information (cyber) security on major international platforms. National communications, particularly in media and scientific discourses, have included frequent narratives consistent with Russia's concept of 'information security' and 'international information security'. Since 2014, Ukraine has significantly strengthened its strategic partnership with the United States and intensified its partnership in cyber security. This has resulted in developing primary national strategic planning documents that set out conceptual positions in line with Western views. At the UN level, Ukraine favoured the draft resolution A/RES/73/266 submitted by the United States. And since the launch of the Programme of Action for Responsible Behaviour in Cyberspace, Ukraine has supported this initiative. This state has also officially announced it will take an active international position in support of Western principles, to strengthen partnerships with stakeholders who share a vision of the future of cyberspace as global, open, free, stable and secure, based on human rights and fundamental freedoms and democratic values.

As of the beginning of the third decade of the 21st century, Ukraine generally demonstrates actions representing the approaches to information security typical of Western countries. However, there is no precise positioning of national policy in this area regarding the strategic priorities of cooperation with major international partners, i.e., the United States, the EU and other NATO member states. Ukraine does not take an active part in the main negotiating tracks at the UN level, particularly within its First Committee. And it does not formulate the state's position in the context of the current UN GGE, neither has it joined the Open-ended Working Group (OEWG). Such participation would be expected if Ukraine chose a clearer position on international cooperation in information security. Despite the strategic course to join the European Union, Ukraine lacks a proactive stance

on the Programme of Action on Responsible Behaviour in Cyberspace, in coordination with decision-making centres in the EU.

In the scientific context, there is a phenomenon of following the narratives, which are widespread in the Russian information field and, in general, correspond to the strategic and foreign policy priorities of Russia, particularly regarding the establishment of an 'international information security' regime. Such concepts as 'national information space', 'information sovereignty', 'information security' etc., which are promoted by authoritarian states, are relevant among scholars and lawmakers in Ukraine. At the level of international platforms and in the area of public diplomacy, international processes of confrontation increase, but Ukraine does not have a sufficient level of adequate scientific and legal analysis of Russia (and China) to promote drafts of international legal acts on international information security. Specifically, it refers to the following issues: the development of rules of conduct; establishing a separate domain of international law in the field of information security; authoritarian governance of the internet; information sovereignty; and a particular concept of combating cyber crime, different from positions set in the Budapest Convention. In this context, one should also expect a more specific idea of information security in domestic information policy in accordance with the state's positions on international platforms, particularly public communication, media and scientific discourses.

In addition, in the area of international cooperation on information security, significant changes are associated with the implementation of foreign policy and global strategies of leading international actors (US, Russia, China, EU). This will result in the need for the careful study of related processes. The intensification of relations between Ukraine and these actors, especially the European Union, is particularly relevant and could be the topic of further research.

References:

Akushev, M. (1999). Information society and legal regulation: new problems of theory and practice. *Information society,* No. 1. Retrieved from http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2be96a4e-09339699c32568b1003ab653

Anichkina, T. (2007). About some techniques of the US information war. *Canada: economy, politics, culture*, No. 7, 123–127.

Averianova, N., & Voropayeva, T. (2020). Information Security of Ukraine: Socio-Philosophical Aspects. *Young Scientist*, No. 10. Retrieved from https://molodyivchenyi.ua/index.php/journal/article/view/319/308

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176–198.

Bykov, I. (2008). Internet governance as one of the problems of modern international relations. *Politèks*, No. 2. Retrieved from: https://cyberleninka.ru/article/n/upravlenie-internetom-kak-odna-iz-problem-sovremennyh-mezhdunarodnyh-otnosheniy

Christou, G. (2014). The EU's Approach to Cyber Security. *EU-China Security Cooperation: Performance and Prospects Policy Paper Series*. Essex: University of Essex. Retrieved from https://www.essex.ac.uk/research-projects/eu-china-security-cooperation/publications.

Council of Europe (2001). *Convention on Cybercrime* (European Treaty Series – No. 185). Budapest: Council of Europe. Retrieved from https://rm.coe.int/1680081561

Digwatch (2021). UN GGE and OEWG. *Digwatch* Retrived from https://dig.watch/processes/un-gge

Doroshko, M. (2017). Ukraine between Russia and the West. *Wschód Europy. Studia humanistyczno-społeczne, 2*(1), 103–112. Retrived from http://dx.doi.org/10.17951/we.2016.2.1.103

ENISA (2022). *The ENISA Threat Landscape 2022*. Retrived from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

EU4Digital (2021, June 7). Cyberspace: EU and Ukraine launch dialogue on cyber security. *EU4Digital.* Retrieved from https://eufordigital.eu/cyberspace-eu-and-ukraine-launch-dialogue-on-cyber-security/

European Commission (2020, December 16). *The EU's Cybersecurity Strategy for the Digital Decade. Joint Communication to the European Parliament and the Council.* Retrived from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

European Media Platform (2015). *Results of discussion within the round table 'Global Internet Governance and the position of Ukraine'*. Retrived from https://eump.org/system/resources/W1siZiIsIjIwMTUvMTIvMDQvMDlfNDdfMTRfOTQyX1N1bW1hcnkuZG9jIl1d/Summary.doc

Farrell, H. (2015). *Promoting Norms for Cyberspace*. New York, NY: Council on Foreign Relations.

Fedorov, A., & Zinovieva, E. (2017). *International Information Security: Political Theory and Diplomatic Practice*. Moscow: Moscow State Institute of International Relations.

Finnemore, M. (2011). Cultivating International Cyber Norms. In K. Lord & T. Sharp (Eds.), *America's Cyber Future: Security and Prosperity in the Information Age* (pp. 89–101). Washington, D.C.: Center for a New American Security. Retrieved from https://www.cnas.org/publications/reports/americas-cyber-future-security-and-prosperity-in-the-information-age

FOIA (2016). Freedom of Information Act Statute. *FOIA.* Retrived from https://www.foia.gov/foia-statute.htm

Frolova, O. (2018). The role of the UN in the system of international information security. *Electronic edition of the Institute of International Relations "International Relations. Part: Political Science*", No. 18–19. Retrieved from http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468

Frolova, O. (2019). International cooperation in the field of information security. *Bulletin of Lviv University. Series: International Relations*, (46), 123–136. Retrived from http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13

Gao, X. (2022, May 27). An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. *The International Spectator, 57*(3) 15–30. Retrieved from https://www.tandfonline.com/doi/full/10.1080/03932729.2022.2074710

Giacomello, G. (Eds.). (2016). *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*. Bloomsbury Academic.

Greenberg, L., Goodman, S., & Soo Hoo, K. (1997). *Information Warfare and International Law.* Washington: National Defense University Press.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155–1175.

Hao, Y. (2017). A Three-Perspective Theory of Cyber Sovereignty. *PRISM, 2*(7), 109–115. Retrieved from https://cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/10-3-Perspective%20Theory.pdf?ver=2017-12-21-110647-937

Havryltsiv, M. (2020). Information security of the state in the system of national security of Ukraine. *Legal scientific electronic journal*, No. 2, 200–203. Retrieved from http://lsej.org.ua/2_2020/54.pdf

Hofmann, J. (2007). Internet Governance: A Regulative Idea in Flux. In R. K. J. Bandamutha, (Eds.), *Internet Governance: An Introduction* (pp. 74–108). Hyderabad: Icfai University Press. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327121

Horlynskyi, V., & Horlynskyi, B. (2019). Cybersecurity as a component of information security of Ukraine. *Information technology and security*, *7*(2), 136–148. Retrieved from https://ela.kpi.ua/bitstream/123456789/33883/1/ITS2019-7-2_03.pdf

Ivančík, R. (2021). Informačná vojna – jeden z multidisciplinárnych fenoménov súčasnej ľudskej spoločnosti. *Politické Vedy, 24*(1), 135–152. Retrived from https://doi.org/10.24040/politickevedy.2021.24.1.135-152

Ivanov, S., & Tomilov, O. (2013, March 14). Cyberterrorism: a threat to national and international security. *IA "Weapon of Russia"*. Retrieved from https://bit.ly/2UFEJl6

Janczewski, L., & Colarik, A. (Eds.). (2008). *Cyber Warfare and Cyber Terrorism*. Hershey, PA: Information Science Reference.

Kisilevych-Chornoivan, O. (2009). Information security and international information security: the problem of defining concepts. *Jurisprudence: theory and practice*, No. 8, 11–18. Retrieved from http://nbuv.gov.ua/UJRN/utp_2009_8_2

Kopiika, M. (2020). Modernization of the policy of international organizations in the field of information security. *Political life*, No. 1, 102–109. Retrieved from https://jpl.donnu.edu.ua/article/view/7967/7967

Korotkov, A., & Zinovieva, E. (2011). Security of Critical Information Infrastructures in International Humanitarian Law. *Vestnik MGIMO-Universiteta*, No. 4, 154–162.

Kostyrev, A. (2010). Political and legal problems of building the system of international information security in the context of globalization. *Modern Ukrainian politics. Politicians and political scientists about this*, (21), 234–246. Retrieved from http://dspace.nbuv.gov.ua/bitstream/handle/123456789/26810/26-Kostyrev.pdf?sequence=1

Krutskih, A. (2007). To the political and legal foundations of global information security. *International processes*, *1*(5), 28–37.

Kucheryavyi, M. (2013). Global Information Society and Security Issues. *Power. National Science and Policy Journal,* No. 9, 89–92.

Kurbalija, J. (2014). An Introduction to Internet Governance. *DiploFoundation*. Retrieved from https://www.diplomacy.edu/resource/an-introduction-to-internet-governance/

Legvold, R. (2022, March 29). The West and Russia Face Tough Choices in Ukraine. *The National Interest*. Retrieved from https://nationalinterest.org/feature/west-and-russia-face-tough-choices-ukraine-201477

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation.

MacLean, D. (Eds.). (2005). *Internet Governance: A Grand Collaboration*. New York, NY: UN ICT Task Force Series.

Madsen, M. D. (2007). *A Fragmented Ukraine: Part of the West or Apart from the West?* (Master's Thesis). Naval Postgraduate School, Monterey, CA. Retrieved from https://core.ac.uk/download/pdf/36696834.pdf

Makarenko, Ye., Ryzhkov, M., Ozhevan, M. et al. (2016). *International information security: theory and practice.* Kyiv: Center for Free Press.

MCIPU (Ministry of Culture and Information Policy of Ukraine) (2020, January 20). *Comparative table to the draft Law of Ukraine "On Amendments to Certain Legislative Acts of Ukraine on Ensuring National Information Security and the Right to Access Reliable Information*. Kyiv: Ministry of Culture and Information Policy of Ukraine Retrieved from https://mkip.gov.ua/files/pdf/Disinformation_Draft_2020.pdf

MFARF (Ministry of Foreign Affairs of the Russian Federation) (2011, September 22). *Convention on International Information Security*. Moscow: The Ministry of Foreign Affairs of the Russian Federation. Retrieved from https://carnegieendowment.org/files/RUSSIAN-DRAFT-CONVENTION-ON-INTERNATIONAL-INFORMATION-SECURITY.pdf

MFAU (Ministry of Foreign Affairs of Ukraine) (2021, June 4). Ukraine and the EU have launched a Cyber Dialogue. *Ministry of Foreign Affairs of Ukraine.* Retrieved from https://mfa.gov.ua/news/ukrayina-ta-yes-zapochatkuvali-kiberdialog

Minesashvili, S. (2022). Ukraine: European Identity Discourses and Elite Relations Under Crises. In S. Minesashvili, *European Identities During Wars and Revolutions. Change under Crisis in Georgia and Ukraine* (pp. 163–249). Palgrave Macmillan, Cham.

Ministry of Defence of the Russian Federation (2011). Conceptual views on the activities of the Armed Forces of the Russian Federation in the information space. *Ministry of Defence of the Russian Federation*. Retrived from https://webcache.googleusercontent.com/search?q=cache:rrxp49KQl1MJ:https://ens.mil.ru/science/publications/more.htm%3Fid%3D10845074%40cmsArticle&cd=10&hl=uk&ct=clnk&gl=ua&client=opera

Molander, R., Riddle, A., & Wilson, p. (1996). *Strategic Information Warfare. A New Face of War.* Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/monograph_reports/MR661.html

Nastyuk, V., & Bielievtseva, V. (2014). Legal bases of international cooperation on counteraction to information offenses. *Pravova* ìnformatika, *2*(42), 40–46. Retrieved from http://ippi.org.ua/sites/default/files/14nvypip.pdf

NATO (2009, September 14). *NATO Strategic Communications Policy* G(2009)0794. Retrived from https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf

NATO (2023). *Allied Joint Publication-10, Allied Joint Doctrine for Strategic Communications* (Edition A Version 1). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1146501/20230328-AJP_10_EdA_V1_Strategic_Communications-O.pdf

Nieles, M., Dempsey, K., & Yan Pillitteri V. (2017). *An Introduction to Information Security* (NIST Special Publication 800-12). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

NISD (National Institute for Strategic Studies) (2014, February 26). *Problems of regulatory and legal support of information sovereignty in Ukraine. Analytical report*. Retrieved from https://niss.gov.ua/doslidzhennya/informaciyni-strategii/problemi-normativno-pravovogo-zabezpechennya-informaciynogo

NIST (National Institute of Standards and Technology) (2022). *Information Security Policy. Glossary.* Retrieved from https://csrc.nist.gov/glossary/term/information_security_policy

NSDC (National Security and Defense Council). (2021). *Cybersecurity Strategy of Ukraine (2021–2025). Secure cyberspace is the key to successful development of the country* (*Draft*). Retrieved from https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

Panarin, I. (2006). *Information warfare and geopolitics*. Moscow: Pokoleniye.

Perm Mission of Ukraine (2021b, June 3). 1 червня відбулося організаційне засідання Робочої групи відкритого складу з безпеки використання інформаційно-комунікаційних технологій у контексті міжнародної безпеки, створеної резолюцією ГА ООН 75/240 від 31.12.2021 на період з 2021 до 2025 рр. [Facebook status update]. Retrieved from https://www.facebook.com/UKRinUN/posts/1598129170538016

Perm Mission of Ukraine to the UN. (2021a, March 13). 12 березня 2021 року Робоча група відкритого складу у сфері інформаційно-комунікаційних технологій (ІКТ) у контексті міжнародної безпеки (Робоча група) під головуванням Постійного представника Швейцарії при Відділенні ООН та інших міжнародних організаціях у Женеві Ю. [Facebook status update]. Retrieved from https://www.facebook.com/UKRinUN/posts/1540234969660770

Pravdiuk, A. (2022). Problems of Legal Regulation of the Information Security System in Ukraine. *European Political and Law Discourse, 9*(2), 40–47. Retrieved from https://eppd13.cz/wp-content/uploads/2022/2022-9-2/07.pdf

President of Ukraine. (2016, March 15). *Cybersecurity Strategy of Ukraine* (No. 96). Kyiv: President of Ukraine. Retrieved from https://www.president.gov.ua/documents/962016-19836

President of Ukraine. (2017, February 25). *Doctrine of information security of Ukraine* (No. 47/2017). Kyiv: President of Ukraine. Retrieved from https://www.president.gov.ua/documents/472017-21374

President of Ukraine. (2021, December 28). *Strategy of Information Security* (No. 685/2021). Kyiv: President of Ukraine. Retrieved from https://www.president.gov.ua/documents/6852021-41069

Romanchuk, Yu. (2009). *International cooperation in the field of information security: conceptual and regulatory aspects:* dissertation abstract, political science. Kyiv: National Academy of Sciences of Ukraine, World Institute. Economics and International relations. Retrieved from http://www.

irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=ARD&P21DBN=ARD&Z21ID=&IMAGE_FILE_DOWNLOAD=1&Image_file_name=DOC/2009/09ryvkra.zip

Rossiyskaya Gazeta (2014, December 25). Military doctrine of the Russian Federation. *Rossiyskaya Gazeta.* Retrived from https://rg.ru/documents/2014/12/30/doktrina-dok.html

Rossiyskaya Gazeta. (2016, December 6). Doctrine of Information Security of the Russian Federation. *Rossiyskaya Gazeta*. Retrived from https://rg.ru/documents/2016/12/06/doktrina-infobezopasnost-site-dok.html

Rossiyskaya Gazeta. (2019, July 5). Federal Law of 1 May 2019 N 90-FZ On Amending the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'. *Rossiyskaya Gazeta*. Retrived from https://rg.ru/documents/2019/05/07/fz90-dok.html

Schmitt, M. (2021, June 10). The Sixth United Nations GGE and International Law in Cyberspace. *Just Security*. Retrieved from https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

Schmitt, M. (Eds.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York, NY:Cambridge University Press.

Schmitt, M. (Eds.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* New York, NY:Cambridge University Press.

Security Council of the Russian Federation. (2021, April 14). *Fundamentals of the state policy of the Russian Federation in the field of international information security* (No. 213). Moscow: Security Council of the Russian Federation. Retrieved from http://www.scrf.gov.ru/security/information/document114/

Sharikov, p. (2018, January 16). Understanding the Russian Approach to Information Security. *European Leadership Network.* Retrieved from https://www.europeanleadershipnetwork.org/commentary/understanding-the-russian-approach-to-information-security/

Shevchuk, O. (2021). Constitutional and legal basis of ensuring information security in Ukraine. *Scientific Bulletin of Flight Academy. Section: Economics, Management and Law*, No. 5,. 209–215. Retrieved from https://fmnzb.sfa.org.ua/wp-content/uploads/2022/01/27.pdf

Shvets, D. (2005*). Information security of the Russian Federation in modern international relations.* Abstract diss. … candidate of sociological sciences. Moscow: MGIMO (U) MID Rossii.

Smirnov, A. (Eds.). (2011). *Global Security: Innovative Techniques for Conflict Analysis*. Moscow: Obshchestvo «Znanie» Rossii.

Solodka, O. (2020b). Information Sovereignty and Information Security of Ukraine: Dialectics of Concepts. *European Political and Law Discourse*, *7*(6), 233–239. Retrieved from https://eppd13.cz/wp-content/uploads/2020/2020-7-6/31.pdf

Solodka, O. (2020a). Ensuring the information sovereignty of the state: legal discourse. *Information and law*, *1*(32). Retrieved from http://il.ippi.org.ua/article/view/200311

Sopilko, I. (2021). Information Security as an Object of Regulation in the Law of Ukraine. *Journal of International Legal Communication*, *1*(1), 11–22. Retrieved from https://jilc.e-science.space/wp-content/v1/JILC01(1).pdf

Szafranski, R. (1995). A Theory of Information Warfare: Preparing for 2020. *Airpower Journal*, *1*(IX), 56–65. Retrieved from https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf

Taylor, E., & Hoffmann, S. (2019). *EU-US Relations on Internet Governance*. *Research Paper*. London: Chatham House. Retrieved from https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf.

The White House (2018, September 18). *National Cyber Strategy of the United States of America*. Washington, DC: The White House. Retrived from https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Tikk-Ringas, E. (ed.) (2015). *Evolution of the Cyber Domain: The Implications for National and Global Security.* London: Routledge, for the International Institute for Strategic Studies.

Turonok, S. (2003). Information and communication revolution and a new spectrum of military-political conflicts. *Politicheskie issledovaniya*, No. 1, 24–38.

U.S. Department of Justice (2015, January 6). *Terrorism Report 2002–2005*. Washington, DC: U.S. Government. Retrieved from https://www.fbi.gov/file-repository/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view

U.S. Department of Justice (2022, October 4). *Privacy Act of 1974*. Washington, DC: U.S. Government. Retrieved from https://www.justice.gov/opcl/privacy-act-1974

UHHRU (Ukrainian Helsinki Human Rights Union) (2007, March 14). Opinion of Council of Europe experts on the draft law on information. *Ukrainian Helsinki Human Rights Union.* Retrieved from https://www.helsinki.org.ua/2007/03/vysnovok-ekspertiv-rady-evropy-schodo-proektu-zakonu-pro-informatsiyu/

UN General Assembly (2015, July 22). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174). Geneva: United Nations. Retrieved from https://undocs.org/A/70/174

UNIDIR (United Nations Institute for Disarmament Research) (2021). Cyber Policy Portal / Ukraine. *United Nations Institute for Disarmament Research*. Retrieved from: https://unidir.org/cpp/en/states/ukraine

United Nations (1967). *International Covenant on Civil and Political Rights*. New York, NY: United Nations. Retrived from https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf

United Nations (1976). International Covenant on Civil and Political Rights. Article 19. *United Nations.* Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

United Nations (1999, January 4). Developments in the field of information and telecommunications in the context of international security (A/RES/53/70). *United Nations* Retrived from https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R

United Nations (2015, January 13). *Rules of conduct in the field of ensuring international information security* (A/69/723/). Geneva: United Nations. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/04/PDF/N1501404.pdf?OpenElement

United Nations (2018a, December 22). *Advancing responsible State behaviour in cyberspace in the context of international security* (Resolution 73/266). New York, NY: United Nations. Retrieved from https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266

United Nations (2018b, December 5). *Developments in the field of information and telecommunications in the context of international security security* (Resolution 73/27). New York, NY: United Nations. Retrieved from https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27&Lang=R

United Nations (2020). *The future of discussions on ICTs and cyberspace at the UN*. New York, NY: United Nations. Retrieved from https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf

United Nations. (2017, October 11). *Draft United Nations Convention on Cooperation in the Field of Combating Information Crime* (Annex to the letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary General). New York, NY: United Nations. Retrieved from https://namib.online/wp-content/uploads/2020/04/Проект-Конвенции-Организации-Объединенных-Наций-о-сотрудничестве-в-сфере-противодействия-информационной-преступности.pdf

UNODA (United Nations Office for Disarmament Affairs) (2021, March 12). Open-ended Working Group. *United Nations.* Retrived from https://www.un.org/disarmament/open-ended-working-group/

UNODA (United Nations Office for Disarmament Affairs) (2023). *Updated Concept Of The Convention Of The United Nations On Ensuring International Information Security*. New York, NY: United Nations.. Retrived from https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf

Verkhovna Rada of Ukraine. (1992). *Law of Ukraine on Information* (No. 48, 650). Kyiv: Verkhovna Rada of Ukraine. Retrieved from https://zakononline.com.ua/documents/show/151399___591468

Verkhovna Rada of Ukraine. (1996). *Constitution of Ukraine*. Kyiv: Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

Verkhovna Rada of Ukraine. (1998a, July 7). *Draft Law on Information Sovereignty and Information Security of Ukraine* (N 1207). Kyiv: Verkhovna Rada of Ukraine. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=4192

Verkhovna Rada of Ukraine. (1998b). *Law of Ukraine on the National Informatisation Program* (No. 27–28, 181). Kyiv: Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text

Verkhovna Rada of Ukraine. (1999, April 15). *Draft Law on Information Sovereignty and Information Security of Ukraine* (N 1207-1). Kyiv: Verkhovna Rada of Ukraine. Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=5871

Verkhovna Rada of Ukraine. (2009, July 8). *Doctrine of Information Security of Ukraine* (N 514/2009). Kyiv: Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/514/2009#Text

Verkhovna Rada of Ukraine. (2010, October 13). *Draft Law on the Concept of State Information Policy* (N 7251). Kyiv: Verkhovna Rada of Ukraine. Retrieved from https://ips.ligazakon.net/document/JF5LF00A?an=3

Verkhovna Rada of Ukraine. (2017). *Law of Ukraine on Cybersecurity* (No. 45, 403). Kyiv: Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text

Verkhovna Rada of Ukraine. (2021, August 26). *Cybersecurity Strategy of Ukraine. Secure Cyberspace – the Guarantee of Successful Development of the Country* (No. 447/2021). Kyiv: Verkhovna Rada of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text

Virchik, G. & Harris, J. (2022, Februray 25). Can Ukrainians Survive East-West Conflict & Their Own Bad Actors? *Convergence*. Retrieved from https://convergencemag.com/articles/can-ukrainians-survive-east-west-conflict-their-own-bad-actors/

Voitsikhovskiy, A. (2020). Information security as a component of the national security system (international and foreign experience). *Bulletin of V.N. Krazin Kharkiv National University. Series "Law"*, (29), 281–288. Retrieved from https://periodicals.karazin.ua/law/article/view/15648/14947

Weber, V. (2023, March 21). The Dangers of a New Russian Proposal for a UN Convention on International Information Security. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security

Wenger, A. (2001). The Internet and the Changing Face of International Relations and Security. *Information and Security*, 7, 5–11.

Zhu, Sh. (2015, December 29). Wuzhen initiative on Internet future. *Shanghai Daily*. Retrieved from https://archive.shine.cn/business/it/Wuzhen-initiative-on-Internet-future/shdaily.shtml