Centre international de formation européenne
Institut européen • European Institute

MASTER IN ADVANCED EUROPEAN AND INTERNATIONAL STUDIES
EUROPEAN INTEGRATION AND GLOBAL STUDIES

THE PRISONERS' DILEMMA OF THE CYBER RELATIONS BETWEEN THE EUROPEAN UNION AND RUSSIA

Anastasiia BOGDANCHIKOVA
Thesis director: George TZOGOPOULOS
Jury Assessor: Frédéric LEPINE

Centre International de Formation Européenne
Master of Advanced European and International Studies, 2021-2022

Acknowledgements

I want to sincerely thank my research advisor, George Tzogopoulos, for accepting me as an advisee. His recommendations helped me develop ideas and to further inspire my line of thinking.

Furthermore, I have the utmost gratitude and affection for CIFE as an institution for allowing me to pursue new facets of global politics. This endeavour would not have been possible without professors and their passion for sharing knowledge, openness to critical thinking, and constant assistance.

Finally, I would like to express my deepest gratefulness to my classmates for accompanying me during this unforgettable journey and for their unconditional support throughout the course in Berlin, Nice, and Istanbul.

PLAGIARISM STATEMENT / *DECLARATION SUR L'HONNEUR CONTRE LE PLAGIAT*

I certify that this thesis is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation. I further certify that I have not copied or used any ideas or formulations from any book, article or thesis, in printed or electronic form, without specifically mentioning their origin, and that the complete citations are indicated in quotation marks.

I also certify that this assignment/report has not previously been submitted for assessment in any other unit, except where specific permission has been granted from all unit coordinators involved, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons.

In accordance with the law, failure to comply with these regulations makes me liable to prosecution by the disciplinary commission and the courts of the French Republic for university plagiarism.

Je certifie que ce mémoire est un travail original, basé sur mes propres études et recherches et que toutes les sources utilisées dans sa rédaction ont été indiquées. Je certifie, de surcroît, que je n'ai ni recopié ni utilisé des idées ou des formulations tirées d'un ouvrage, article ou mémoire, en version imprimée ou électronique, sans mentionner précisément leur origine et que les citations intégrales sont signalées entre guillemets.

Je certifie également que ce mémoire n'a pas été précédemment soumis pour évaluation dans une autre unité, sauf si une permission spécifique a été accordée par tous les coordinateurs d'unité impliqués, et que je n'ai pas copié en partie ou en totalité ou autrement plagié le travail d'autres étudiants et/ou personnes.

Conformément à la loi, le non-respect de ces dispositions me rend passible de poursuites devant la commission disciplinaire et les tribunaux de la République française pour plagiat universitaire.

Name/*Nom*: Anastasiia Bogdanchikova

Date: 15.06.2022

Signature:

Abstract

Russian Federation and the EU are two critical players in the international arena on the cyber subject matter. Even though both actors participate in multilateral platforms dedicated to creating a harmonised cyber governance, one can notice few signs of cooperation in practice. Moreover, headlines connecting Russia to some offensive operations against EU member states have become a daily bread for their bilateral relations agenda. This paper argues that even though the EU and Russia do not have official combating interests in cyberspace, both clashes and cooperation are possible. The current stalemate reminds of a prisoner's dilemma. It will be applied as a theoretical approach to analyse the evolution of EU-Russian relations and offer four paths to its future development.

This report seeks to clarify the difference between cyberspace and information space approaches in the EU-Russian strategic thinking. It analyses the cyber policies of two actors from the end of the 20th Century until the beginning of 2022, both on domestic and international levels, and explores how these governance systems contradict, overlap, or match each other. The report examines four possible outcomes in EU-Russia relations by applying the prisoner's dilemma theory. Finally, based on specifics of the current international situation, it evaluates the most probable outcome and offers several policy recommendations for addressing harmonised and prosperous activities in cyberspace for the future.

Table of contents

List of abbreviations

AI	Artificial Intelligence
ASN	Autonomous system numbers
BRICS	Brazil, Russia, India, China and South Africa
CBM	Confidence-building measures
CCDCoE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CII	Critical information infrastructure
CIS	Commonwealth of Independent States
COVID-19	Coronavirus disease 2019
CoE	Council of Europe
CSTO	Collective Security Treaty Organisation
DDoS	Distributed denial of service
DG	Directorate-General
DGA	Data Governance Act
DMA	Digital Markets Act
DNS	Domain name servers
DoS	Denial of service
DSA	Digital Services Act
EDA	European Defence Agency
EEAS	European External Action Service
ENISA	European Network and Information Security Agency
EU	European Union
EUCSS	EU Cyber Security Strategy
Europol	European Police Office
FSB	Federal Security Service of the Russian Federation
GDP	Gross domestic product
GDPR	General Data Protection Regulation
GGE	Group of Governmental Experts
GRU	Main Directorate of the General Staff of the Armed Forces of

	the Russian Federation
ICT	Information and communications technology
Interpol	International Criminal Police Organization
IR	International relations
IT	Information Technology
ITU	International Telecommunication Union
MFA	Ministry of Foreign Affairs
NIS Directive	Directive on security of network and information systems
NATO	North Atlantic Treaty Organization
OPCW	Organisation for the Prohibition of Chemical Weapons
OSCE	Organisation for Security and Cooperation in Europe
OEWG	Open-ended working group
PCA	Partnership and Cooperation Agreement
PESCO	Permanent Structured Cooperation
R&D	Research and development
SCO	Shanghai Cooperation Organisation
StratCom	Strategic Communication Task Force
UN	United Nations
UNGA	United Nations General Assembly

Any comment or information only
engages the responsibility of the author.

Introduction

Cyberspace is everywhere, and it is an empirical fact. Today not only our computers are connected to the World Wide Web, but also cars, houses, watches, and other everyday devices. Modern International relations (IR) evolve together with humanity. As the Digital Revolution took place, states and international actors also started interacting in cyberspace. This state-to-state engagement is a rapidly developing reality of contemporary IR that created a new dimension[1]. The world has become interconnected through cyberspace, but at the same time, it has become dependent. Without this technology business, public service, and water supply can no longer be efficiently provided. Therefore, it is evident that while creating endless opportunities, cyberspace has become a threat to national, private, and individual security. Today, cybersecurity is an issue of top priority discussed both by academics and political elites of many countries.

The European Union-Russian relations emerged in 1992 following the collapse of the Soviet Union and the advent of the European Union (EU). Thenceforth, parties have fairly shared difficulties. There are several approaches to interpreting the nature of these relations, whether evolved because of changes within the EU, Russia, or events outside the EU and Russia's control. Nonetheless, the EU-Russia relationship is rich and diversified, even though it is frequently reduced to its most controversial components of various connections and interdependencies. Indicating a gap between the legal basis and practice analysis of EU-Russian relations, it remains unclear what are the possible consequences of these relations in the near future. Therefore, **the research question of this work is the following: what are the potential implications of the EU-Russia cyber relationship?**

[1] Farwell, J., Rohozinski, R. (2012). 'The New Reality of Cyber War', Survival, vol. 54 no.4, pp. 107-120.

This thesis aims to outline various understandings of the current EU-Russia cyber relations and explore them in multi-temporal, multi-perspectival, and multi-level terms. Based on the domestic and international legislation and practice of the two actors, this thesis aims to develop a comprehensive perspective on policies in the cyber domain and to determine the possibilities of both clashes and cooperation between them.

Regarding the methodology, this thesis uses analytical research to build a case regarding the future of EU-Russian relations, based on each party's historical and legal background. Through a comparative analysis, this paper examines both actors' strategic vision of cyberspace and information space governance and the possibility of reinforcing or aggravating each other. The thesis offers potential tracks for developing these relations by applying these findings to the prisoner's dilemma matrix.

Many scholars focused their scientific interest on cybersecurity in international relations. However, no research provides advice on the strategic development of relations in this sphere after February 2022. This thesis is supported and emphasised by a wide range of resources, including official laws, analyses, press releases, and newspaper reports. This approach to the literature provides doublechecked facts and a broad perspective on the issue through solid arguments. This comprehensive approach to resources provides viewpoints of both actors and puts them on the canvas of the global context.

The most valuable sources on the theory of cybersecurity in international relations are written by J.S. Nye[2], S.N. Romaniuk and M. Manjikian[3], B. Valeriano and R. C. Maness[4], and J.-F. Kremer and B. Müller[5]. There are no significant works

[2] Nye, J. S. (2010). 'Cyber Power'. Harvard Kennedy School.

[3] Romaniuk, S.N., Manjikian, M. (2021). 'Routledge Companion to Global Cyber-Security Strategy'. London: Routledge.

[4] Maness, R.C., Valeriano, B. (2018). 'International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain', in Brown, C., Eckersley, R. (eds.) The Oxford Handbook of International Political Theory.

[5] Kremer, J.-F. and Müller, B., 2013. 'Cyberspace and International Relations'. Heidelberg, : Springer Berlin.

on the latest events that occurred between the EU and Russia in this area, although there are remarkable researches on these relations up to 2018[6,7].

This thesis will be composed of four chapters. **In Chapter I**, the paper explores cybersphere and information sphere concepts to explain how these terms relate to each other both from an academic and a political point of view. That allows contextualising the study topic before introducing the prisoner's dilemma approach to a research design. The study demonstrated that the prisoner's dilemma theory explains the two parties shared concerns about various issues.

Chapter II provides a context and reasoning for Russian cyber management based on its national interests and subordinating private interests within the state's agenda. The chapter presents how the Russian government prefers to safeguard and manage its information space rather than its cyber infrastructure and aims to promote these ideals worldwide. This chapter focuses on three dimensions of Russian infosecurity: internal, strategic, and international. Applying these dimensions to the global context, the chapter explains why and how the Russian infosphere's protective divergence deepens from the global one.

Chapter III provides an overview of cyber affairs in the European Union, interprets the nature of challenges to ensure coherence between EU member states, and describes the influence of union policies in the global arena. Following a brief history of cyber threats to the EU's supranational stability, the chapter discusses the evolution of strategy and cybersecurity measures over the previous decade. The chapter then explores issues in maintaining coherence amid changing technology and political conditions and recent initiatives for cyberspace legislation. In the end, the chapter gives an outlook of Europe's norm-based digital foreign policy that advanced both its external and domestic sovereignty, as well as intensified aspirations for deeper European integration.

Chapter IV explores the practical applications of EU-Russian ties on bilateral and multilateral bases from the end of the 20th Century up till today. The

[6] Hernández i Sagrera, R., Potemkina, O. (2013). 'Russia and the common space on freedom, security and justice', CEPS Paper in Liberty and Security in Europe.

[7] Limnell, J. (2018). 'Russian cyber activities in the EU', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 65–75.

chapter investigates the overall vector of affairs in specific topics of cyber terrorism and the development of global norms of behaviour. Further exploring the context of bilateral relations, the chapter provides a broad context of cyber operations and mutual accusations. In the end, the chapter offers the application of the prisoner's dilemma to thesis findings, ranging from highly likely to highly unlikely scenarios.

Finally, the last chapter provides **the conclusion** of the work applying the model with the research results to today's global context, highlighting factors required for the development of the EU-Russian strategic communication in addressing activities in cyberspace. The paper offers recommendations for the EU and Russia on how to deepen cooperation on cyber domain issues.

Chapter I: Theoretical framework

The cyberspace itself was created neither secure nor resilient. The original idea of the Internet was to create an open, user-friendly, generative, and advanced democratic substrate, following the liberal ideas of IT enthusiasts in the 1990s[8]. The openness of cyberspace made it much easier to expand five offence advantages traditionally held only by emperors or superpowers: the vastness of resources, large armies, the ability to move great distances, the application of a wide variety of weaponry over time, the immunity of the home base[9]. Any actor with access to the Internet and time can execute cyber campaigns with minimal expense. The shared context of the interconnected infrastructure creates a need for an appropriate response to such threats. In addition to technical aspects, the complexity of the virtual environment shapes its management and is manifested through it. A. Barrinha and T. Renard examine the idea of cyber diplomacy as an attempt to construct an international cyber society, mixing together national interests with world society dynamics[10]. Diplomats became more included in cyber issues as these issues became more politicised.

To detect and describe the correlates of cyberspace, it is important to consider their theoretical implications. This chapter focuses on cyberspace and its security and how academics define it and distinguish it from information security.

1.1 Overlap of cyberspace and the information sphere

The approach to understanding cyberspace is not unilateral. In the scientific literature, cyberspace is usually associated just with the Internet; however, it is not restricted within the scope of the World Wide Web. Multiple frameworks have been elaborated to understand cyberspace. According to F. Kramer, there were up to 28 definitions of "cyberspace"[11]. Many scholars divide cyberspace into

[8] Geer, D. et al. (2003). 'Cyberinsecurity: The cost of monopoly'.

[9] Demchak, C.C. (2012). 'Cybered conflict, cyber power, and security resilience as strategy', in Reveron D. (ed.), Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Washington, DC: Georgetown Press, pp. 121-136.

[10] Barrinha, A., Renard, T. (2017). 'Cyber-diplomacy: the making of an international society in the digital age', Global Affairs, vol.3 no.4-5, pp. 353–364.

[11] Kramer, F. (2009). 'Cyberpower and national security: POLICY recommendations for a strategic framework', in Kramer, F., Starr, S., Wentz, L. (eds), Cyberpower and National Security. Dulles: Potomac Books, pp. 3–23.

technological/physical (hardware), logical (software), and human networks. For example, according to Z. Trejnis and P. Trejnis, "cyberspace encompasses all information and communication means in a collection of networks, techniques, users and digital space, which in turn is assigned three layers: material, logical and informational"[12]. In this chapter and further in this work, the cybersphere will be understood as this broad concept, including technology, infrastructure, users, and content they create.

The different understanding of cybersphere, cybersecurity, and information sphere and infosecurity concepts between Western countries in contrast to states such as Russia and China triggers instability in international politics. The lack of a shared context, comprising principles and norms holds back the development of harmonised global cyberspace and cybersecurity mechanisms.

The Russian Federation has no direct definition of cyberspace. However, one can find quite a lot of literature in Russian on the way the Russian government defines the "information sphere" – a term that includes both technical aspects of processes in cyberspace and the content part[13]. This term is used and promoted by Russian officials in domestic and foreign policy.

The EU uses the word "cyberspace" as a term but does not have a clear definition of it in official documents. Usually, the context of legal acts focuses on cyberspace as a global domain that includes an interdependent network of information infrastructures, including the Internet, telecommunication networks, and computer systems.

According to the Copenhagen school of thinking, cybersecurity is the result of the combination of technology, procedures, and everyday habits. It focuses on how diverse actors employ various representations of risk to develop or transform various governmental, private, societal, and commercial understandings of security in certain public realms[14]. Therefore, the difference between the Russian approach

[12] Trejnis, Z., Trejnis, P. (2017). 'Polityka ochrony cyberprzestrzeni w państwie współczesnym', Studia Bobolanum, vol. 28 no. 3, p. 27.

[13] Fridman O. (2017). 'The Russian perspective on Information Warfare', Defence Strategic Communications, Vol. 2, pp. 75-76.

[14] Cavelty, M.D. (2022). 'Cybersecurity between hypersecuritization and technological routine', in Tikk, E., Kerttunen, M. (eds.) Routledge Handbook of International Cybersecurity. New York: Routledge, pp. 11-21.

to the information sphere and the European approach to the cybersphere do not contradict each other and can be compared.

The cyberspace is critical for the interconnection of industries and the government. Regulators develop rules that are compatible with technological progress, and industry proposes goods that are compatible with high-level vision[15]. Those who control the hardware and software also determine which innovations and business models are applicable and who can access data. That triggers the spread of the global competition between liberal democracies and authoritarian systems. While Western countries, including the EU, see cybersecurity as a combination of data protection, freedom of cyberspace, and trustworthy digital technologies, Russia and China set a goal of putting the main focus on the state's involvement in shaping, watching, and governing the Internet and the content. That is why for these two countries the information is primarily important rather than the network itself.

The cyberspace is increasingly often used as the "fourth battleground"[16]. Lawson shows in his cybersecurity analysis that there is a widespread application of the "war" analogy when discussing cyberspace[17]. That led to approaching cyber through a realism lens as a military threat. Cybersphere allows the application of a similar containment strategy during the Cold War, which provoked the application of deterrence strategies: preventing someone from doing something by convincing them that the expenses will outweigh the benefits. For example, political scientist J. S. Nye contends that, opposing common opinion, deterrence can occur in cyberspace. He believes that the creation of an international ruleset, which has been undeveloped, can have a vastly beneficial impact. International norm-making procedures can also deter state actors from attacks. Furthermore, the deterrence in cyberspace is different from the nuclear one. It requires not just the threat of punishment but also denial by the defence (to build resilient systems that attackers

[15] Hunker, J. (2012). 'Policy Challenges in Building Dependability in Global Infrastructures', Computers & Security, no. 21, pp. 705-711.

[16] Stone, A. (2011). 'Cyberspace: The next battlefield', USA Today, June 19.

[17] Lawson, S. (2012). 'Putting the 'war' in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States', First Monday, vol.17 no.7, pp. 49-73.

will not bother to try) and entanglement (creating tools that any attack will likely harm the interests of offenders)[18].

1.2 Prisoner's dilemma and international relations

The prisoner's dilemma theory is a vital game theory that has been introduced into military, political, and economic issues for its insights. This theory, which was first applied as a mathematical approach in the past century, began to be used to analyse war and peace between countries[19]. The prisoner's dilemma theory in international relations helps to clarify actors' decision-making strategies toward one another. It explains the difficulty decision-makers confront in international politics[20]. As soon as states seek greater advantages while experiencing the fewest losses while interacting, game theory assists decision-makers in reaching the most balanced win-loss ratio in a particular situation. It explains why, even though the best-case scenario is evident, rational actors acting in self-interest can allow the worst-case situations to occur.

There are three possible outcomes in the prisoner's dilemma theory: the "win-win" scenario, the "zero-sum" equation, and the worst "negative-sum" outcome, where both sides lose[21]. Both parties must interact within specific strategies and consider the necessity of gaining new advantages over the other party[22]. Strategy implementation is one of the sides of rational behaviour. However, as nations' intentions toward one another remain hidden; therefore, state decision-makers cannot forecast what the other states intend to do[23].

In 1992, Albert Tucker presented a situation in which two prisoners had two alternatives influencing the prison sentence. Tucker's example is illustrated in the

[18] Nye, J.S. (2021). 'The End of Cyber-Anarchy?', Foreign Affairs, December 14.
[19]Snidal, D. (1985). 'The game theory of international politics', World Politics, vol. 38 no. 1, pp. 25-37.
[20] Correa, H. (2001). 'Game theory as an instrument for the analysis of international relations' 立命館国際研究, vol.14 no.2., pp.187-208.
[21]Lake, D. (2013). 'Theory is dead, long live theory: The end of the great debates and the rise of eclecticism in international relations', European Journal of International Relations, vol. 19 no.3, pp. 567-587.
[22] Tema, M. (2014). 'Basic assumptions in game theory and international relations', International Relations Quarterly, vol.5 no.1, pp. 1-5.
[23] McCarthy, M. (2014). 'The role of games and simulations to teach abstract concept of anarchy, cooperation, and conflict in world politics', Journal of Political Science Education, no.10, pp. 400-413.

Table I[24]. It shows that if each prisoner betrays the other, he will receive a larger pay-off.

TABLE I. TUCKER'S PRISONER'S DILEMMA

	Prisoner B stay silent (cooperates)	Prisoner B betrays (defects)
Prisoner A stay silent (cooperates)	Both serve 1 year	Prisoner A serves 3 years, Prisoner B goes free
Prisoner A betrays (defects)	Prisoner A goes free, Prisoner B serves 3 years	Both serve 2 years

Lack of trust and the fear of betrayal pushes both convicts to testify against each other, even though cooperation is more favourable.

The realism theory of international relations describes a similar scenario between governments that are frequently sceptical of one another despite previously negotiated agreements. One of the basic principles of international relations indicates that states are mainly concerned about their benefits and, as far as possible, seek to maximise their advantages. K. Waltz and J. Geico, representatives of the Realism school of thought, explain this tendency by emphasising that country's primary goals are independence and security. Scientists further describe how states respond to not simply the potential, but the possibility of threats presented by other states[25,26].

Notably, the prisoner's dilemma in international relations may be applied to the cyber realm to illustrate the difficulties of cyber interferences and how actors might cope with these new necessities in the global arena. If an international actor announces its capabilities, its adversaries may begin working on countermeasures; for example, when nations begin developing offensive and defensive cyber capabilities and intent to create a cyber unit within armies. Furthermore, states have begun to employ cyberspace to achieve their objectives since the Internet provides a political cover through proxy servers and the usage of non-state players. It has

[24] Poundstone, W. (1992). Prisoner's Dilemma. NY: Doubleday, p.8.

[25] Geico, J., 1988, 'Realist Theory and the Problem of International Cooperation: Analysis with an Amended Prisoner's Dilemma Model', The Journal of Politics, vol. 50 no.3, p. 601.

[26] Waltz, K. (1979). Theory of International Politics. Reading, Mass.: Addison-Wesley Pub. Co.

proven to be dangerously useful, given the lack of international rules and regulations targeted at punishing potential offenders. Such cyber anarchy and distrust between countries pose enormous obstacles to collaboration, as shown by the prisoner's dilemma.

The prisoner's dilemma theory may clarify many past and ongoing examples of disputes or competition in the world arena, including Russia and the EU. This study will apply the prisoner's dilemma theory to the EU-Russian rivalry in the cyber and information spheres, demonstrating how relevant and significant this theory is in both actors' decision-making.

Chapter II: The Russian approach to cyber-sovereignty

Russian Federation builds its cybersphere regulation design around firm commitments to national interests. Usually, private and individual interests are submitted to governmental ones. In contrast to the Western or liberal, the Eastern concept of cyber-sovereignty justifies such measures. Echoing the Chinese approach, Russia aims to protect its cyberspace by controlling an information discourse rather than cyber infrastructure. Russia tries to promote the same ideas and values in the international arena.

To understand the Russian approach to infosecurity, this chapter will focus on domestic, strategic, and international domains. While sub-parts of the chapter focus on three domains separately, the Table II follows the narrative and summarises all these dimensions to create a zoom-out perspective. Developments in all domains are interconnected with historical events and the global context, which is also reflected in the table. Additionally, the table includes cyber operations that are supposed to be or were conducted by the Russian government.

A reader can observe the deepening of the separation of the Russian infosphere from a global one. Russian politics in the sphere becomes more protective domestically while promoting the same governing pattern and values abroad.

2.1 Terminology of the Russian approach

Though cybersecurity is a disputable term for many politicians today, it has not been applied on an official level in Russia. There are several definitions of ICT usage, and Russia prefers to discuss information security (or infosecurity) rather than cyber derivatives. That is due to more than solely linguistic differences, it also reflects a conceptual gap in cyber approaches.

The most frequent definition of cybersecurity pertains to the operational and infrastructure level of information exchange rather than the content itself. The concepts of confidentiality, integrity, and availability define the common

TABLE II. RUSSIAN CYBER APPROACH IN THREE DOMAINS

Global context	Domestic legislation	Strategic vision	Foreign policy	Cyber operations

1991 – Gulf War coalition's success;
1999 – Second Chechen War;
Colour revolutions;
		2000 – Doctrine on Information Security.	**1998** – resolution on "Developments in information and telecommunications in the context of international security",
			the UN GGE meetings.
			2001 – Budapest Convention;
			2005 – EU-Russian Road Map for the Common Space on Freedom, Security, and Justice.
			
			Narratives: prohibition of "information weapons";
			global coordination of law enforcement agencies.	

2008: Munich speech,
War in Georgia;
2011-2013 – Moscow protests;
2011 – Arab spring.
	2012 – Internet Blacklist;
	2012 – Foreign Agents Law;
	2013 – Prosecutorial Internet blockage.
		2013 – Prototype Concept of Cybersecurity Strategy.	**The mid-2000s** – UN GGE meetings.	**2014** – Ukraine (elections, critical infrastructure).

2014 – Crimea annexation.	**2014:** Dissemination of Historical Narratives,
	Law on Bloggers,
	Law on data localization,
	Law on Foreign ownership of media companies;
	2016 – "Yarovaya" package of laws;
	2017 – Legislation regulating messenger services;
	2019 – Sovereign Internet law.
		2015 – National Security Strategy;
		2016 – Doctrine on Information Security;
		2016 – Foreign Policy Concept.
			2015 – Code of Conduct for information security;
			2017 – Draft UN Convention on Cooperation in Combating Cybercrime;
			2019 – Countering the use of information and communication technologies for criminal purposes resolution to replace the Budapest Convention;
			2020 – establishment of OEWG.
			2021 – UN GGE consensus on cyber behaviour.
			
			Narratives:
			The development of an international infosecurity system pursues the establishment of international legal frameworks.
				2015 – Germany (parliament);
				2016 – US (elections);
				2017 – France (elections);
				2014 – WADA/sports organisations;
				2018 – Winter Olympic Games;
				2019 – Georgia (parliament, media);
				2021 – healthcare system of Ireland.

2022 – War in Ukraine	**2022 –** Foreign Agents Law update		**2022** – China and Russia joint statement on sovereign right to regulate national segments of the Internet.	

cybersecurity triad. It implies that information is only accessible to the intended users, accurate and complete, with no breaches or unauthorised modifications, and that information can be accessed anytime. D. B. Parker expanded the triad and included three more principles: possession or control, authenticity, and utility[27]. The first principle emphasises maintaining control over information since its loss endangers security. The second principle addresses the originality of authorship. Finally, utility implies that information is still usable after all other security precautions have been taken. The Russian model focuses primarily on information security, leaving infrastructure as a default component. That leads to a conclusion that the Russian official narrative excludes the term "cybersecurity" but refers to "information security"[28]. Also, it is the reason why there is no legislation concerning equipment and the organisation of the cyber market. Further examination of official government doctrines will assist in defining information security and tracking the term's development.

Russia focuses on the digital environment as "information space" or "information sphere", which is considered broader than the Western concept of "cyberspace" or "cyber domain". The definition of the information sphere is defined in Russia's Doctrine of Information Security from 2016 as follows:

> *"a combination of information, informatisation objects, information systems and websites within the information and telecommunications network of the Internet [...], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating social relations in the sphere"*[29].

[27] Parker, D. B. (2014). 'Toward a New Framework for Information Security', in S. Bosworth, M. E. Kabay & E. Whyne (eds.), The Computer Security Handbook (6th ed.). New York: Wiley, chapter 3.

[28] Hakala, J., Melnychuk, J. (2021). 'Russia's strategy in cyberspace'. NATO Strategic Communications
Centre of Excellence.

[29] Russian Federation (2016a). 'Doctrine of Information Security of the Russian Federation', Decree of the President of Russian Federation from 05.12.2016 N646 [Указ Президента Российской Федерации от 05.12.2016 г. N 646].

As a result, Russia approaches the information space as a geopolitical term, indicating its domestic information space with a representation of Russian territorial borders[30].

2.2 Development of Russian infosecurity approach

Russian ideas on the use of information have evolved due to experiences made inside and outside the country. On the one hand, the Soviet Union started attracting attention to a so-called "Revolution in Military Affairs" in the 1980s, influencing fighting through informatisation. On the other hand, calls for revolution during the 1991 Gulf War were widely ignored by the Soviets, which led to the coalition's success. As a result, the significance of information technologies was gradually recognised. The Central Federal government dominated the traditional media channels during the Second Chechen War in 1999. However, they could not overturn the global impression of courageous independence war, as the rebels used the Internet to portray themselves as heroes.

As a result, in 2000, Russia developed its first Doctrine on Information Security[31]. It is a comprehensive document that formulates the concept of infosecurity from the angle of national security, with the national interest playing a significant role. Russia's infosecurity is a platform of interest of the state in the field of ICT, defined by the total sum of individual, social, and national (state) interests. From there, we may discover the cornerstone triad of infosecurity: individual, society, and state. This triad is critical for understanding Russian perceptions of infosecurity risks and Russian policies for its implementation.

There are four distinguished national interests in the 2000 doctrine[32]:

1) freedom and access to information;
2) access to open governmental info resources for citizens;
3) modern ICTs production and export of these products;

[30] Kukkola J., Ristolainen M. (2018). 'Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders', Journal of Information Warfare, vol. 17 no. 2, pp. 83- 100.

[31] Russian Federation (2000). 'Doctrine of Information Security of the Russian Federation', Decree of the President of Russian Federation from 09.09.2000 N PR-1895 (invalid)[Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 г. N Пр-1895) (утратила силу)].

[32] See above, part I, article 1.

4) information and data protection.

Noticeably, international cooperation for infosecurity was also emphasised in several ways. The first sector is related to the prohibition of the development, proliferation, and use of "information weapons"[33]. Secondly, Russia highlights guarantees of secure information exchange and the security of data when it is being transmitted through national telecommunication networks. Another objective was the global coordination of law enforcement agencies' activities to prevent digital crimes, unauthorised access to information from law enforcement agencies, and the fight against international terrorism, drug smuggling and distribution, illegal weapons trade, and people trafficking. International cooperation also included the security of international financial telecommunication networks. Russia established closer ties with the Commonwealth of Independent States (CIS) in the infosecurity domain to accomplish these objectives. Later, Russia ensured full involvement in all international organisations working in the field, including standardisation and certification of infosecurity measures.

The doctrine's last section described how infosecurity policies should be implemented: it allocates authority between legislative, executive, and judicial branches on the federal and regional levels[34]. As a result, the state is the most critical stakeholder in infosecurity politics. It analyses Russia's infosecurity threats; manages federal information defence agencies; supports public organisations; controls the development and trade flows of infosecurity tools through certification; protects domestic producers and the federal market; encourages global access to information resources and networks; fosters the country's entry into the global information community based on an equal partnership.

With the progress of ICT and political events inside and outside Russia, the infosecurity strategy of 2000 has lost relevancy. The 2008 Russian-Georgian war, 2011-2013 Moscow protests over illegitimate elections and the role swap between Vladimir Putin and Dmitry Medvedev highlighted how social media might incite public unrest. The Arab upheavals had proved the power of social networks in

[33] See above, part II, article 7.
[34] See above, part IV.

regime change, adding to the Kremlin's concern that something similar would happen in Russia[35].

In the meantime, before the revised strategy's release in 2016, a prototype Concept of Cybersecurity Strategy in Russia was made public in 2013[36]. It attempted to merge the concepts of cybersecurity and infosecurity into a valuable strategy for Russia. In contrast to the doctrine of 2000, the goal was to close current loopholes in cybersecurity law in Russia and to provide the footing for the engagement of civil society and the private sector together with state entities. Cybersecurity here is defined as a "set of conditions in which all components of cyberspace are safeguarded against the greatest number of threats and impacts with unfavourable outcomes". Surprisingly, the document was the first to present the Concept of multistakeholderism at such a high political level. The proposal's basic principles included, among others, the notion of "the constructive cooperation of all subjects of the information society – individuals, companies, and the state – in cybersecurity". That encourages the division of responsibilities among actors: the state conducts regulation of cybersecurity and coordinates stakeholders; the private sector ensures the security of critical infrastructure under their ownership through complying with cybersecurity standards, and society would have to increase digital literacy and provide feedback on the state and business efforts. Even though the Concept contains several progressive ideas for cybersecurity development, it has been condemned by the business for the ambiguity and uncertainty of its provisions, as well as by state officials, who claim that it "contradicts state policy in this field"[37]. Following the State Duma hearings on the Concept at the end of 2013, the Security Council was required to examine it for future implementation. However, the project's fate is unclear, and there is reason to doubt that it either got stalled in the approval stage or was rejected. At the 6th Russian Internet Governance Forum in 2015, the working group's chairman commented on the Concept that he would no

[35] Giles, K. (2016). ' Russia's 'New' Tools for Confronting the West'. London: Chatham House, the Royal Institute of International Affairs, pp. 29-31.

[36] Russian Federation (2013a). 'Concept of Cybersecurity Strategy, project'.

[37] Chernenko, E., Ivanov, M. (2013). 'The concept of cybersecurity has diverged from the state strategy. So far, only public figures and businesses like the senators' proposals [Концепция кибербезопасности разошлась с государственной стратегией. Предложения сенаторов нравятся пока только общественникам и бизнесу]'. Kommersant, November 29, no.220, p. 2.

longer pursue this initiative because the significant aim had been met – the public debate and legislative activity had been sparked and ongoing.

At the end of 2016, the new "Doctrine on Information Security" was approved and signed[38]. The introduction section states that the Doctrine is aimed for a strategic planning in the national security sphere, and it develops the provisions of Russia's national security policy released in 2015[39]. The foundation triad of an individual, society, and the state remained in the Doctrine. The Russian national interests in cyberspace included "objectively significant needs of an individual, the society and the state in ensuring their security and sustainable development in the area of information". National interests, from a more detailed view, include a set of goals divided into five areas[40]:

1) *content security*, to ensure people's constitutional rights and freedoms to access and use information; privacy protection; information support to institutions, to provide mechanisms of interaction between the state and civil society; and to ensure Russia's multi-ethnic population's cultural, historical, and spiritual values.

2) *infrastructure cybersecurity* to ensure the resilience of Russia's essential information infrastructure and its telecommunications network in peacetime and conflict.

3) *development of technological potential* to grow Russian ICT and enhance digital instruments' creation, manufacture, and operation.

4) *international security* of information to provide credible information on the state's official position in Russia and throughout the globe.

5) *principle of sovereignty*, to counter the ICT threats undermining strategic stability and the protection of Russian sovereignty in infospace.

[38] Russian Federation (2016a).

[39] Russian Federation (2015). 'National Security Strategy of the Russian Federation', Decree of the President of Russian Federation from 31.12.2015 N 683 [Указ Президента Российской Федерации от 31.12.2015 г. N 683].

[40] See above, Doctrine of Information Security of the Russian Federation, 2016: Part II, article 8.

Part III of the Doctrine addresses the Russian government's primary concerns about infosecurity. The Doctrine identifies the following dangers and challenges[41]:

1) application of cross-border information flow for illegal geopolitical, terrorist, and extremist activities.

2) ability of other nations to influence Russia's information infrastructure for military purposes.

3) psychological influence through information flows to destabilise political and social institutions, challenging other governments' sovereignty and territorial integrity.

4) increasing biases in foreign media towards Russian state policy and discrimination against Russian journalists overseas.

5) computer crimes and privacy violations.

6) violation of international law through ICT to threaten international peace and undermine Russia's sovereignty, political and social stability, and territorial integrity.

As a result, the Doctrine grants a leading role to the state in providing infosecurity. Nevertheless, the strategy includes other participants: owners and operators of critical information infrastructure, media, sectors of the financial market, service providers, ICT developers, and education and civil society organisations. Thus, the Doctrine captures the multistakeholder idea while leaving each stakeholder's scope of obligations and capabilities undefined. Meanwhile, the Doctrine establishes governmental principles to foster constructive partnership between state, organisations, and citizens to solve infosecurity problems. It balances citizens' needs for free information exchange and issues of national security insurance.

The Doctrine also highlights the degree of imported ICT dependency, which causes security concerns, and the low rate of national R&D projects. Furthermore, the worldwide allocation of resources required for safe and reliable Internet connection does not allow equal Internet governance. Finally, the lack of

[41] See above, Part III.

international cyber norms and mechanisms for their application makes it challenging to form an international infosecurity system aimed at achieving equal strategic partnership[42].

The strategy offers a set of actions to minimise risks and counter the abovementioned problems[43]. From a military politics perspective, it is the prevention and containment of infospace conflicts, the growth of capacities to conduct information combat, and the protection of Russian allies' interests in infospace. Secondly, in the realm of state and public security, the strategy calls for the defence of sovereignty, political and social stability, territorial integrity, as well as the provision of fundamental human rights and freedoms and the safeguarding of essential information infrastructure. For economic, science, and technology development, the strategy calls for an expansion of the digital economy in the national GDP rate, substitution for foreign ICT goods, development of an infosecurity pool of professional personnel, and popularisation of personal infosecurity culture.

The primary goal of international cooperation is to establish a stable system of peaceful inter-state relations in the information domain. To achieve this goal, Russia would implement an autonomous strategy to ensure national objectives to protect its sovereignty. Russia will actively engage in the development of an international infosecurity system, fighting against the use of ICT for military and political reasons in violation of international law. That means that Russia would pursue the establishment of international legal frameworks to avoid and resolve interstate conflicts in cyberspace. Third, Russia will advocate for equal and mutually beneficial collaboration among all interested players in the information field at multilateral organisations.

At the end of the Doctrine analyses, it should be noted that despite providing a detailed description of information security threats, none of them was named. It has not pointed at other countries, or terrorist groups, or blamed the Western world for the imbalanced governance of Internet resources.

[42] See above, Part III.
[43] See above, Part IV, article 21.

2.3 National cybersecurity legislation

The government's approach toward the Internet and cyberspace has evolved in the last ten years. Previously, the Russian Internet and digital services could be described as self-organised, self-regulated, and not interfered by the state. Right after post-election protests in the winter of 2011, the Parliament passed legislation controlling the broadcast of information on the Internet. During this period Russian government introduces laws to influence the information sphere inside the country. In 2012, the Internet Blacklist (139-FZ)[44], a central blacklist that may be enforced without a court order, and the Foreign Agents Law (121-FZ)[45] to regulate and limit the scope of political activities of any organisation that receives funding outside Russia. In 2013, Prosecutorial Internet blockage (398-FZ)[46] that gives the Prosecutor General the authority to block any website without a trial if it seemed to contradict Russian legislation. In 2014, with the Dissemination of Historical Narratives (128-FZ)[47], the government used historical narratives of the Soviet World War II legacy to mobilise the population to support the Kremlin's foreign policy and Crimea annexation. The Law 97-FZ[48] has required bloggers with over 3000 followers to indicate themselves to authorities and hold responsibility for comments by any other user under their posts. Furthermore, this law obliged Internet services allowing sending messages, to keep voice, text, images, sounds,

[44] Russian Federation (2012b). Federal Law 'On Amendments to the Federal Law 'On the Protection of Children from Information Harmful to Their Health and Development' and Other Legislative Acts of the Russian Federation' dated 28.07.2012 N 139-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'О защите детей от информации, причиняющей вред их здоровью и развитию' и отдельные законодательные акты Российской Федерации' от 28.07.2012 N 139-ФЗ].

[45] Russian Federation (2012a). Federal Law 'On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Regulation of the Activities of Non-Commercial Organizations Acting as Foreign Agents' dated 20.07.2012 N 121-FZ [Федеральный закон 'О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента' от 20.07.2012 N 121-ФЗ].

[46] Russian Federation (2013b). Federal Law 'On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection' dated 28.12.2013 N 398-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'Об информации, информационных технологиях и о защите информации' от 28.12.2013 N 398-ФЗ].

[47] Russian Federation (2014d). Federal Law 'On Amendments to the Certain Federal Law' dated 05.05.2014 N128-FZ [Федеральный закон 'О внесении изменений в отдельные законодательные акты Российской Федерации' от 05.05.2014 N 128-ФЗ].

[48] Russian Federation (2014b). Federal Law 'On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection' and Certain Legislative Acts of the Russian Federation on Regulating the Exchange of Information Using Information and Telecommunication Networks' dated 05.05.2014 N 97-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'Об информации, информационных технологиях и о защите информации' и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей' от 05.05.2014 N 97-ФЗ].

or other electronic messages for up to six months within Russian territory. Law on the Foreign ownership of media companies (305-FZ)[49] does not allow non-Russian investors to own more than 20% of a media company operating in Russia.

Another federal law that caused a headache for Internet providers was the protection of data of Russian residents and the physical location of this data within Russian borders (242-FZ)[50]. Not all international Internet powerhouses have met the standards for organising the storage and processing of a person's data in Russian data centres. For example, LinkedIn was banned from using on the territory of Russia for non-compliance[51].

In 2016, the President approved amendments to federal anti-terrorism legislation and the Criminal Code, nicknamed the "Yarovaya package"[52,53]. Regarding infosecurity, the package has obliged ICT providers to keep correspondence and user data. Furthermore, it requires providers of mass communication services to decrypt users' messages. Companies are forced to submit keys to encrypted traffic at the request of the Federal Security Service of the Russian Federation (FSB). Telegram Messenger declined to give encryption keys, stating that confidential discussions in Telegram employ end-to-end encryption. However, that justified the decision to prohibit the messenger on the Russian

[49]Russian Federation (2014c). Federal Law 'On Amendments to the Law of the Russian Federation 'On the Mass Media' dated 14.10.2014 N 305-FZ [Федеральный закон 'О внесении изменений в Закон Российской Федерации 'О средствах массовой информации' от 14.10.2014 N 305-ФЗ].

[50] Russian Federation (2014a). Federal Law 'On Amendments to Certain Legislative Acts of the Russian Federation for Clarifying the Procedure for Processing Personal Data in Information and Telecommunication Networks' dated 21.07.2014 N 242-FZ [Федеральный закон 'О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях' от 21.07.2014 N 242-ФЗ].

[51] BCS Express (2017). 'LinkedIn leaves Russia [LinkedIn уходит из России]'.

[52] Russian Federation (2016c). Federal Law 'On Amendments to the Federal Law 'On Countering Terrorism' and Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Measures to Counter Terrorism and Ensuring Public Security' dated 06.07.2016 N 374-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'О противодействии терроризму' и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности' от 06.07.2016 N 374-ФЗ].

[53] Russian Federation (2016b). Federal Law 'On Amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure public security' dated 06.07.2016 N 375-FZ [Федеральный закон 'О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности' от 06.07.2016 N 375-ФЗ Federal Law].

territory, by a fact, which never happened. The messenger was "unblocked” officially in 2020[54].

In 2017, the Parliament issued Law FZ-187[55] on the security of Russia's critical information infrastructure (CII). The legislation defined objects (physical equipment of essential infrastructure), actors, and their legal obligations. The bill also amends the Criminal Code (issued as FZ-194[56]) to introduce criminal prosecution for illegal activities against CII items.

That is important to highlight that the growth of national governance of the Russian part of the Internet is one of the most controversial initiatives. Published in 2019, the law focuses on regulating the national sector of the Internet and defending it from foreign threats through centralised Internet traffic routing. Because of its very restricted and fragmented form, people nicknamed it "the Law on Sovereign RuNet"[57]. In essence, the legislation names actors accountable for the stable functioning of the World Wide Web in Russia. Among them are telecom operators, the owners of technical communication networks, traffic exchange points, communication lines, and autonomous system numbers (ASN). All actors are required to participate in regular exercises to ensure the stability of the RuNet. Roskomnadzor, the Russian watchdog for communication, information technology, and mass communications, is to carry out centralised management of communication networks, defining core policy principles for telecom operators. Telecom providers are obligated to implement state-sponsored technical tools in their networks to prevent threats to the stability, security, and integrity of Internet

[54] Gerasyukova, M. (2020). 'Restrictions lifted: Roskomnadzor unblocked Telegram [Ограничения сняты: Роскомнадзор разблокировал Telegram]', Gazeta.ru, June 18.

[55] Russian Federation (2017e). Federal Law 'On the security of the critical information infrastructure of the Russian Federation' dated 26.07.2017 N 187-FZ [Федеральный закон 'О безопасности критической информационной инфраструктуры Российской Федерации' от 26.07.2017 N 187-ФЗ].

[56] Russian Federation (2017d). Federal Law 'On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Code of Criminal Procedure of the Russian Federation in connection with the adoption of the Federal Law 'On the Security of the Critical Information Infrastructure of the Russian Federation' dated 26.07. 2017 N 194-FZ [Федеральный закон 'О внесении изменений в Yголовный кодекс Российской Федерации и статью 151 Yголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона 'О безопасности критической информационной инфраструктуры Российской Федерации' от 26.07.2017 N 194-ФЗ].

[57] Russian Federation (2019). Federal Law 'On Amending the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection' dated 01.05.2019 N 90-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'О связи' и Федеральный закон 'Об информации, информационных технологиях и о защите информации' от 01.05.2019 N 90-ФЗ].

activities on the Russian territory. These technical tools will also be used to filter traffic and avoid access to forbidden Internet resources. Finally, the legislation calls for the establishment of a Russian national domain system to guarantee the limitless accessibility of Russian websites even in case of isolation. This allows complete control of cyberspace in Russia, including managing information flows within and outside the country. This policy largely follows the Chinese approach with their "Great Firewall of China” project. Although the law was supposed to start functioning in November 2019, it is still not ready for execution due to the lack of required directives and decrees governing the technical intricacies.

Since the beginning of the war in Ukraine or, according to the Russian official rhetoric "special military operation”, the pressure on the infosphere has increased. The State Duma adopted an updated version of the Foreign Agents Law. According to this initiative, any person or organization, that is suspected to be "under the influence from abroad", cannot organize public events, conduct educational activities, etc[58].

As it is clear from the context above, the national information security regulation is given the most significant attention. It is the goal of the state to regulate information flows and filter out unwanted content at any cost. Since the first law on critical information infrastructure was adopted some years ago, Russia's government has been working on completing the legislation that seeks to regulate the RuNet infrastructure in the event of a crisis and make it independent of foreign shutdowns. When it comes to virtual sovereignty, the government must not only announce it but also enforce its execution and match the Internet with its national borders[59].

2.4 International domain of infosecurity

Since 1998, Russia has encouraged and been a pioneer of worldwide infosecurity policy. Russia presented a resolution on "Developments in information and telecommunications in the context of international security" to the United

[58] State Duma of the Russian Federation (2022). Legislation initiative No. 113045-8 'On control over the activities of persons under foreign influence' [Законопроект № 113045-8 О контроле за деятельностью лиц, находящихся под иностранным влиянием].

[59] Mueller, M. (2017). 'Will the Internet Fragment? Sovereignty, Globalization and Cyberspace'. London: Polity.

Nations (UN) Secretary-General concerning the increasing challenge of international infosecurity. It emphasised the need to prevent the information sphere from becoming a new battlefield. It also suggested that UN member states should annually report to the Secretary-General about their opinion on the military usage of ICT, the definition of "information weapons" and "information warfare", and the necessity of international legal norms against the development of information weapons. Since the resolution was approved without a vote, the Secretary-General presents yearly reports to the General Assembly on these subjects[60].

The second component of the Russian proposal was the formation of the Group of Governmental Experts (GGE). Its idea was to investigate current and potential hazards emerging from the cyber domain and to identify an appropriate multilateral approach to combat them. The UN GGE has been holding meetings from 2004 to 2021.

During the group meeting in 2015, Russia proposed the updated International Code of Conduct for information security, co-sponsored by Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan[61]. The Code notes the need for new "moral and behavioural norms" in the cybersphere and the concept of "cyber-sovereignty". The fact that the Code originated from the Asian domain proves the "coming together" tendency in Russia-China relations, applicating similar approaches and values to policy. Many Western countries, including the European Union member states, dismissed the Code, interpreting it as an attempt to justify greater state control of the Internet and online content.

In the spring of 2017, Russia made another contribution to the United Nations – the Draft UN Convention on Cooperation in Combating Cybercrime[62]. The text prioritised the protection of state sovereignty: "This Convention shall not authorise a State party to exercise in the territory of another State the jurisdiction and functions that are reserved exclusively for the

[60] UNGA (1999). 'Developments in the field of information and telecommunications in the context of international security'. UNGA A/RES/53/70.

[61] UNGA (2015a). 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General'. UNGA A/69/723.

[62] UNGA (2017). 'Letter dated 11 October 2017 from the permanent representative of the Russian Federation to the United Nations addressed to the Secretary-General'. UNGA A/C.3/72/12.

authorities of that other State under its domestic law". The Convention requires party-states to take legislation and other measures to define criminal acts in the cybersphere, as well as processes to prevent, suppress, investigate, and prosecute such crimes. Article 27 mandates that nations implement real-time traffic data collection, which can be interpreted as bringing their population under surveillance. There are many aspects of the Convention that are unacceptable for democratic nations. The paper did not get any support at that time.

At the 73rd session of the United Nations General Assembly (UNGA), Russian Foreign Minister Sergey Lavrov reaffirmed Russia's intention to negotiate a new cybercrime convention[63]. In 2019, Russia filed a new resolution titled "Countering the use of information and communication technologies for criminal purposes", which was approved by a vote[64]. It requires the Secretary-General to publish at the 74th session of the UN General Assembly a report on member states' perspectives to fight against the use of ICTs for criminal purposes. Some scholars claim this resolution sought to replace the Budapest Convention on Cybercrime with a new convention, creating a new agenda for the next session of the United Nations. Associations for progressive communications attacked the resolution for its use of the vague term "use of ICTs for criminal purposes", which might imply the criminalisation of all online activity in general, and, de facto, Russian national cyber and infosecurity is evolving in this direction:

> *"[...] specifically, cybercrime laws are being applied in ways that stifle dissent and government criticism, outlaw peaceful protests, gain indiscriminate access to people's data, and crack down on tools that enable encryption and anonymity".*
>
> *APC, 2019*[65]

[63] MFA of Russian Federation (2018d). 'Foreign Minister Sergey Lavrov's remarks at the 73rd session of the UN General Assembly, New York, September 28, 2018'.

[64] UNGA (2019b). 'Resolution Countering the use of information and communications technologies for criminal purposes' UNGA 74/247.

[65] APC (2019). 'UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online'.

The latest report of UN GGE in 2021 sealed the consensus on some crucial points. First of all, international law should be also applied online. Secondly, there are 11 norms of state behaviour and how to implement these norms[66]. The Russian delegation was pleased with the 2021 report since encouraging responsible state behaviour is essential to its Information Security Strategy. Despite these encouraging aspects, the report makes modest progress on the application of international law online and the engagement of multiple stakeholders. While the document confirms that international law must be applied in the online world, it fails to specify how it does so. Instead, it encourages governments to contribute their ideas on the matter, leaving unfulfilled legal concerns.

Authoritarian governments mainly share Russia's Internet vision because it allows Internet providers, many of whom are state-owned, to monitor any device linked to the network. China and Russia signed a joint statement on February 4th, 2022, stating that "any attempts to limit their sovereign right to regulate national segments of the Internet and ensure their security are unacceptable, are interested in greater participation of the International Telecommunication Union in addressing these issues"[67].

The International Telecommunication Union (ITU), the United Nations organisation for ICT technologies, is another path for influencing global cyber governance. Another opportunity for Russia comes in September 2022, when the ITU elects a new secretary-general at the Plenipotentiary Conference, with Russia nominating one of the candidates, Rashid Ismailov[68].

The foreign policy of Russia towards international governance reflects the domestic approach of information sovereignty. During the past decade, Russia and China were coming together, applicating similar approaches and values to policy sector by sector, and the cybersphere was not an exemption. That is why countries try to support each other or act together on the agenda of cyber and information security, creating an ally with a solid political say. The war in Ukraine, which

[66] UNGA (2021). 'Developments in the field of information and telecommunications in the context of international security', UNGA 76/135.

[67] Russian Federation (2022). 'Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development'.

[68] Bertuzzi, L. (2022). 'China, Russia prepare new push for state-controlled internet'. EURACTIV.com, February 28.

started in 2022, cut down ties between Russia and the West, leading to cyber-dependency on Chinese equipment in the future.

Chapter III: Supranational experiences and Foreign digital policy of the European Union

The EU prioritises cybersecurity as a policy issue[69]. Networks and network-enabled vital infrastructures have been underlined repeatedly in statements made by EU officials. The language used in major policy documents highlights cybersecurity as a foundation of EU economic and political progress. Millions of EU citizens use billions of Internet-connected devices daily to do business, participate in politics, and, most importantly, for the nature of the EU, communicate across regional, national, and linguistic boundaries.

The extent of the Union's supranational constitution, in large part, and the idea of technological sovereignty dictates the nature of EU cybersecurity concerns and policy approaches. Much as in other sectors, the coherence of policy purpose and outcomes across all parts of the Union and beyond its borders is the primary focus of institutions developing novel approaches wrapped under the "digital" label. However, as A. Barrinha and H. Farrand-Carrapico[70] point out, the importance of coherence for the EU is more than just the traditional need to square expectations and approaches across the naturally broad surface area of continental bureaucracy (i.e., horizontal integration) and membership landscape (i.e., vertical integration)[71]. Instead, the need for coherence comes from a need to make sure that everyone understands the same thing about the nature of cybersecurity challenges, the extent of EU responsibilities in the field (both toward member states and toward private industry), and the potential flexibility for both to evolutionate[72,73]. Even though cybersecurity is a problem area that is probably best described by how different and changing it is, there is a lot of pressure on the EU to make policies that are easily adaptable to variable circumstances and environment. This is especially true because of the need to

[69] European Parliament and Council of the European Union (2016). 'Directive (EU) 2016/ 1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union'.

[70] Barrinha, A., Farrand-Carrapico, H. (2018). 'How Coherent Is EU Cybersecurity Policy?', LSE European Politics and Policy (EUROPP) Blog.

[71] Nuttall, S.(2005). 'Coherence and Consistency', in C. Hill & M. Smith (eds.), International Relations and the European Union, Oxford: Oxford University Press, pp. 91–112.

[72] Cremona, M. (2008). 'Coherence through Law: What Difference Will the Treaty of Lisbon Make?' Hamburg Review of Social Sciences, vol.3 no.1, pp. 11–36.

[73] Pomorska, K. & Vanhoonacker, S. (2016). 'Europe as a Global Actor: Searching for a New Strategic Approach', Journal of Common Market Studies, vol.53 no.1, pp. 216–229.

protect the single market and the euro and the political integrity of supranational institutions whose credibility has been under attack in recent years.

This chapter focuses on the evolution of the EU cybersecurity, including the challenge of cohesion and standard-making. The EU's standard-making influence in digital foreign policy is drawn from its market's strength. That is proven every time when non-European cyber businesses adjust their terms of service to ensure access to the European internal market.

3.1 Early stages of the EU cybersecurity policy

While many Western countries can point to some early experiences of cyber threats that were especially painful, the European Union felt pressure to act on cyber issues primarily because of economic threats rather than geopolitical ones. In the spirit of the European experiment, EU officials have turned their attention to cybersecurity risks to sustain prosperity and economic potential. In addition to early experiences of malicious codes such as Conficker and ILoveYou, the EU has taken note of assaults on intellectual property and essential infrastructure. Worm-enabled ransomware assaults like WannaCry and NotPetya have lately pushed the EU to new heights of cyber cooperation. These attacks were nearly epidemic in their spread throughout sectors of European society, causing billions of euros in damage and urging the EU for its most recent set of attempts to simplify and make a strategic vision for a safe Europe online cohesive.

Over the last two decades, because of the wide range of potential policy approaches, the general public has often perceived cybersecurity as either an obscure issue or just an extension of the earlier emphasis on communications technology as an economic driver. As a result, the Union first focused on cybersecurity solely within an additional framework of the fundamental economic strategy of the 1990s. Several initial documents were noteworthy, notably the White Paper on Growth, Competitiveness, and Employment. The Report on Europe and the Global Information Society[74] and the Challenges and Ways Forward into the Twenty-First Century[75] – identified information technologies as critical to the growth of European markets, the development of the fundamentals of the single market, and the robust maintenance of Europe's innovation economy. The role of information in guaranteeing stability across the EU was a central determinant. Nonetheless, the early EU focus on cyber concerns

[74] Bangemann Group (1994). 'Report on Europe and the Global Information Society', Bulletin of the European Union, Supplement 2/94.

[75] European Commission (1993). 'Growth, Competitiveness, and Employment. The Challenges and Ways Forward into the 21st Century'.

reflected a preference for the coherence of economic aims and outcomes above significant social or political motives.

As noted previously, few big cybersecurity events significantly influenced the EU policy until at least the late 2000s. The emergence of cybercrime in the 1990s (criminal conduct that became strikingly frequent among the Europeans with the expansion of personal Internet connection) motivated measures to better balance the web's development with governance obligations. Consideration of harmful online activity triggered a wave of Union-level initiatives to harness member state capabilities and increase consumer awareness of potential cyber threats. During this time, which lasted until at least the mid-2000s, emphasis was placed on the coordination of knowledge for member state populations, the development of standard definitions of cybercrime, and the standardisation of language to reach a consensus on what a secure web-enabled society in Europe should look like.

The mid-2000s were a turning point for the EU cyber policy, as the Western world battled with the perception that global terrorism, defined by the use of organised crime and other proxy actors, was the most imminent danger to international security[76]. The Global War on Terror, in particular, pushed the European Union to reconsider the legitimacy of policymaking approaches that promoted distributed governance over centralised management[77]. With international terrorism and organised crime, typically related to violent foreign political actions, it became evident that member-level solutions would often not be enough. Such dangers are likely to be transnational, targeting European society in general. For example, EU member states in Eastern and Southern Europe were far less developed than the original members in western Europe regarding the resources and structures necessary to coordinate an effective response, information sharing, and other activities. Even though every state in the Union wanted to fight effectively against non-state and non-traditional threats to European security, these differences made it hard for the EU to protect European society.

By 2003–2004, these problems and the related weaknesses of member-level solutions were recognised as directly linked to cybersecurity. EU officials were particularly worried about how individual member states' regulations on cybercrime and user rights may differ substantially[78]. As a result, the EU's cybersecurity approach shifted

[76] European External Action Service (2017). 'Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy'.
[77] Trauner, F., Carrapico, H. (2012). 'The External Dimension of Justice and Home Affairs after the Lisbon Treaty: Analyzing the Dynamics of Expansion and Diversification', Foreign Affairs Review, no. 17, pp. 1–18.
[78] Van Vooren, B. (2012). EU External Relations Law and the European Neighbourhood Policy. A Paradigm for Coherence. London: Routledge.

dramatically, notably from non-binding supranational coordinating mechanisms to legally binding ones.

Since the mid-2000s, the EU's cyber strategy has been heavily focused on the protection of vital infrastructure and the mitigation of cyber-criminal risks, with a decreased dependence on member state solutions in favour of unified organization-determined ones.

Before 2014, the danger of politically motivated industrial assaults from hostile foreign nations drove the EU's policy focus on cyber protection. EU officials saw the large amount of malicious activity that led to the theft of terabytes of valuable industrial and government data in the early 2010s, especially the "Gh0st RAT" series of intrusions, as a clear and present threat to the continent's economy. Similarly, the rising usage of harmful code to produce real disruptive results presented European stakeholders with a danger that was directly related to transnational terrorism. Stuxnet, a damaging worm used at Iran's nuclear enrichment plant at Natanz, alarmed Europe's cybersecurity community. Not only was the result of a cyberattack tangible, but the code itself was generic, creating the possibility for modifying the virus against any industrial control system[79]. This added to the growing consensus that the scope and nature of cybersecurity threats had changed to the point where they were no longer "low" politics. Instead, cybersecurity was a multi-level issue. Therefore, the EU was especially missing a uniting supranational element.

The early emphasis on cyber defence focused on two primary areas of activity: the development of crisis response coordination (and the way how the EU should be engaged) and the enhancement of national cyber capabilities[80]. Over the next three years, EU entities such as the European Defence Agency (EDA) and the European Commission sought to establish various projects aimed at hardening EU capabilities and coordinating defence across member states. The relationship between these efforts was defined in the EU Cyber Security Strategy (EUCSS) published in 2013[81]. The Strategy aimed to encourage member states to adopt comprehensive roadmaps for the development of defensive capabilities, filtering cyber response into crisis response infrastructures, generating and maintaining robust education opportunities, and creating synergistic initiatives. Significant focus was placed on formal collaboration between the EU and NATO, particularly cooperation

[79] Lindsay, J. R. (2013). 'Stuxnet and the Limits of Cyber Warfare', Security Studies, vol.22 no.3, pp. 365–404.

[80] Pupillo, L., Griffith, M., Blockmans, S., Renda, A. (2018). 'Strengthening the EU's Cyber Defence Capabilities', CEPS Task Force Report.

[81] European Commission (2013). 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'.

between the EDA and NATO's Cooperative Cyber Defence Centre of Excellence (CCDCoE).

The EU acknowledged the need to identify and recover from complex digital threats, in addition to the obvious requirement to respond to emergencies[82]. From 2016 to 2018, the Union made considerable progress establishing these cybersecurity capabilities. The Permanent Structured Cooperation (PESCO) framework was ratified in 2017 by participants from 25 of the 28 (that time) national military forces of EU member states[83]. PESCO's objectives are based on the premise that community responses to cyber threats are likely to increase overall resilience and crisis response results. To this purpose, PESCO signatories committed to the established procedures for creating Cyber Rapid Response Teams and improved platforms for information exchange.

Despite several potential advances in cyber defence, the European Union's reaction to cyber threats from a supranational security perspective remains relatively divided. As M. Griffith writes, EU capabilities remain somewhat segmented among agencies and organisations whose objectives and coordination tasks are not always well defined by law and policy. The response duties of members under the Treaty on the EU are a remarkable issue that remains to this day. Article 42(7) (on mutual assistance) does not define "armed aggression" in a way that makes it possible to tell the difference between large-scale service attacks against a member state, and others, like intrusions that lead to the espionage of sensitive intellectual property[84]. In circumstances when there is no identifiable threat actor, it is unclear where the assistance of other member states lies (albeit the "solidarity clause" of the Treaty for shared security action against terroristic threats). Cyber defence remains fragmented because a lot of effort has been dedicated to the development of standardised approaches that regulate digital society. This is partly because of the top-down approach of the EU, which tries to make it fit into a holistic approach to all of the EU's cybersecurity problems.

3.2 Integration, cohesion and conditions on the ground

Since the middle of the 2000s, the European Union has been building the institutional capacity to deal with cybersecurity broadly. This goes beyond the narrower scope of cyber defence issues. Over the period of 20 years, the EU has built a solid and diverse ecosystem of agencies with different parts of the cybersecurity mission. This

[82] European Commission (2017). 'State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks'.

[83]European External Action Service (2022). 'Permanent Structured Cooperation (PESCO) – Factsheet'.

[84] Pupillo, L., Griffith, M., Blockmans, S., Renda, A. (2018).

includes the EDA and Directorate-General (DG) for Migration and Home Affairs, which oversee different cybercrimes, as well as the DG for Communications, Content, and Technology, the European Network and Information Security Agency (ENISA), and all of the Computer Emergency Response Teams (CERTs).

In many respects, EU institutional development on cyber problems has prioritised coordination over quick infrastructure upgrades. Since 2004, when ENISA was established, the emphasis has been on the cohesion of the EU approach as an essential precursor to the broader protection of Europe's digital society. According to H. Carrapico and A. Barrinha, this effort to establish cohesiveness has progressed along at least two lines: horizontal and vertical integration. First, the EU has worked to create the institutional ecosystem required for protecting European society online[85]. This has prompted the EU to establish many specialist institutions, ranging from ENISA to International Criminal Police Organization (Interpol), tasked with investigating cybercrime[86]. Second, the EU has worked to ensure that everyone is on the same page on the scope and objectives of the European cyber mission. In the context of member states, i.e., horizontal relationships, this has meant efforts to balance policy instruments and national laws, as well as ensuring that approaches to coordination with the private sector are supported by EU institutions. This has resulted in more than a decade of effort focused on aggregating and combining understandings of the Internet's influence on European society. The requirement to produce and sustain a shared meaning in cyber governance discourse has enabled the evolution of methods for accommodating and influencing national cyber objectives.

Overall, it is understandable that the EU's emphasis on cohesiveness above effectiveness has resulted in a gradualist cyber policy environment. Many aspects of the Union's approach to cyber concerns are determined by international frictions that provide barriers not seen in other major world polities. While public-private collaborations on cyber concerns are complex, EU agencies have experienced unique challenges. The EU has typical challenges of mismatched public-private interests (especially on data sharing) and minimal historical engagement in loosely coupled infrastructure sectors (such as Internet technologies). It is also compelled to play a multi-level game with national governments who, although wishing progress on cybersecurity issues, are politically unwilling to regulate private enterprise.

[85] Carrapico, H., Barrinha, A. (2017). 'The EU as a Coherent (Cyber) Security Actor?', Journal of Common Market Studies, vol. 55 no.6, pp. 1254–1272.

[86] Biscop, S., Andersson, J. (2008). 'The EU and the European Security Strategy: Forging a Global Europe'. Abingdon: Routledge.

3.3 NIS Directive, ENISA and the EU cybersecurity act

The EU's gradualism on cybersecurity affects effectiveness in several areas. As soon as the EU's cyber ecosystem has so many different parts, agencies like ENISA, Interpol, and EDA often do not have enough resources or do not have access to the right resources. Moreover, communication barriers remain high among EU stakeholders and counterparts in member states[87].

Nonetheless, some significant initiatives have recently been done to mitigate these issues. Directive 2016/1148 (from now on, the "NIS Directive") was released in July 2016 to standardise cyber threat mitigation across member states further[88]. It offered the first official definitions of the categories of operators, kinds of private business players, and types of acts that should be handled by state regulation[89]. It required national authorities to implement these frameworks through publishing relevant plans, establishing regulation and enforcement bodies (where they did not already exist), and adhering to specified national practice requirements (such as data breach notification).

The NIS Directive promotes ENISA, the EU's cybersecurity agency, to a far more crucial position in maintaining continental cybersecurity than previously. According to the Directive, ENISA is solely responsible for providing EU support to member nations and ensuring member states' compliance with the Directive[90]. ENISA must give the necessary knowledge to member state agencies and assist in the developing of any public-private collaboration guidelines to be used by the Cooperation Group (the EU support sub-unit). Furthermore, the Directive made ENISA an advisor, requiring the agency to consult the EU Commission before taking official action. These mandates, combined with the agency's new role to assist in appointing representatives at various levels of coordination, place ENISA at the centre of all decisions concerning the development of the EU's coordinative cyber workforce and the distribution of necessary resources. ENISA is also positioned to define more cohesive strategic ideas in the future. The EU Cybersecurity Act, passed in mid-2019, strengthens ENISA's position at the forefront of EU cyber policy enforcement by requiring the agency to be the only permanent authority for various operational-level efforts[91]. Finally, the implications of cybersecurity action in the EU in the framework of

[87] Carrapico, H., Barrinha, A. (2017).
[88] European Parliament and Council of the European Union (2016).
[89] Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation'. Computer Law and Security Review, vol. 35 no.6, pp. 1-11.
[90] See above.
[91] European Commission (2019). 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)'.

the General Data Protection Regulation (GDPR) are streamlined by these directives[92]. The GDPR, enacted with the NIS Directive, is a wide-ranging legislative act aiming to improve data security for European residents. In cases when both pieces of law apply, such as when personal data is uncovered during a data breach response, ENISA's presence at the core of Europe's cyber policymaking promises to provide order where there may have been uncertainty.

3.4 Further development of the EU cyber legislation

In 2020, the EU adopted a new Cybersecurity strategy as a core pillar of Shaping Europe's Digital Future, the Recovery Plan for Europe, and the EU Security Union Strategy[93]. The strategy aims to boost collective security among its member states based on reliable services and digital tools and increase the adaptation capacity. With this strategy, Brussels expects not only to strengthen the domestic cyber infrastructure but to lead on international norms and standards in cyberspace and expand global partnership, promoting a European approach. New Cybersecurity Strategy will be sponsored by investment from Digital Europe Program, Horizon Europe, and the Recovery Plan for the EU. Initiatives include the creation of a new Cybersecurity Emergency Response Fund.

All further initiatives find their basis in this strategic vision.

The resilience of European networks is to be developed by the diversification of backbone infrastructure, including the recently launched initiative for secure satellite communications through the Union Secure Connectivity Programme mechanism for 2022-2027, announced in February 2022[94].

The Commission also proposed to establish a network of Security Operations Centres covering the EU, able to discover early evidence of a cyberattack to enable instant response.

In March 2022, the European Commission proposed up-to-date guidelines to implement common cybersecurity and information security measures across the Union. The cybersecurity regulation will create a new interinstitutional Cybersecurity board and strengthen the to be renamed CERT-EU (from "Computer Emergency Response Team" to "Cybersecurity Centre"). The proposed Information Security Regulation will define a

[92] European Commission (2016). 'Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)', Official Journal of the European Union.

[93] European Commission (2020b). 'Joint Communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade'.

[94] European Commission (2022h). 'Proposal for a Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2022-2027'.

minimum set of regulations and standards for all EU institutions to secure information exchange[95].

In May 2022, The EU legislators reached a trialogue agreement (not the formal approval at the time of publication) on the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) – flagship cybersecurity legislation, proposed by the Commission in December 2020[96]. To respond to Europe's increased exposure to cyber threats, the NIS 2 Directive now requires a broader scope of medium and large entities, organisations, and industries to manage cybersecurity risk. The new expanded standards will boost cybersecurity by requiring more organisations and industries to manage cybersecurity risks. The legislation includes public electronic communications services, digital services, wastewater and waste management, and central and regional public administration. Considering the COVID-19 pandemic, it also includes medical device makers. The NIS 2 Directive increases enterprises' cybersecurity standards and certification, covers supply chain and supplier security and holds senior management accountable for noncompliance. It simplifies reporting responsibilities, adds tighter supervisory and enforcement procedures, and tries to harmonise punishment regimes across the member states.

In 2022, the Commission launched a public discussion on cyber resilience[97]. This legislation will introduce uniform cybersecurity guidelines for producers and suppliers of tangible and intangible digital products and associated services to fulfil market demands and safeguard consumers against unsecure products. Official adoption of the initiative by the Commission is planned for the third quarter of 2022.

As a part of the Cybersecurity strategy, the union will expand efforts to constantly improve the workforce, recruit the most talented cybersecurity personnel, and invest in open, competitive, and excellence-based research and innovation.

In 2022, the Council of the EU presented the new Strategic Compass, which is, among other activities, designed to strengthen "all at once" EU member states' situational awareness in the cybersphere[98]. According to the document, the EU will call for internal and external cybersecurity agencies to prepare pooling their intelligence in the European External Action Service (EEAS) in case of necessity.

[95] European Commission (2022g). 'New rules to boost cybersecurity and information security in EU institutions, bodies, offices and agencies'. Press release.

[96] European Commission (2022d). 'Commission welcomes political agreement on new rules on cybersecurity of network and information systems'. Press release.

[97] European Commission (2022c). 'Commission invites citizens and organisations to share their views on the European Cyber Resilience Act'. Press release.

[98] Council of the European Union (2022). 'A Strategic Compass for Security and Defence'.

3.5 EU sovereignty in the cyber age and digital foreign policy

In the recent decade, the EU has had considerably accomplished in exporting its standards and guidelines in the realm of digital foreign policy. The Brussels Effect, described by A. Bendiek and I. Stürzer, is founded on the assumption that disagreements originating from various interpretations of essential norms by states may be successfully resolved by manoeuvring with private participants on the digital market [99].

Brussels Effect has an internal and exterior dimension, emphasising that the EU's normative influence is the fundamental weapon for European diplomacy. Internally, the EU may provide advice on complex questions including, for example, responsibility for the platform economy and data protection of open sources, such as social media platforms. From a foreign policy point of view, the EU can mainstream its basic principles and standards by establishing the criteria necessary for entry to the internal market. Therefore, the "Brussels Effect" relates at the same time at three directions: member state, European, and international levels. The updated model of the "effect" of the EU cyber policy is described in the Table III.

The Brussels Effect in the digital sphere originates from a segmented and comprehensive approach to legislation. The first segment of the cyber policy – internal market standards – includes the European e-commerce directive[100], Digital Services Act (DSA)[101], and Digital Markets Act (DMA)[102]. The European e-commerce directive specifies norms for service provider transparency, responsibility along the business chain, including intermediate service providers, and commercial communications laws. The DSA announced additional guidelines on transparency, including the collection and commercialization of user data, addressing expressions of hatred and intolerance, restrictions for users, and reporting on those publishing unlawful content. The DMA aims to establish the field for businesses of "gatekeepers" – huge Internet platforms.

The second segment defines the structure and values of the cybersphere. The NIS Directive[103], which defines international norms in the digital sphere by limiting entrance to the EU market, was the first step toward forming a uniform EU digital foreign policy. In

[99] Bendiek, A., Stürzer, I. (2022). 'Advancing European Internal and External Digital Sovereignty', Stiftung Wissenschaft und Politik.

[100] European Commission (2000). 'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')'. Official Journal of the European Union.

[101] European Commission (2022f). 'Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment'. Press release.

[102] European Commission (2022e). 'Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets'. Press release.

[103] European Parliament and Council of the European Union (2016).

2019, EU Cybersecurity Act created a system of cybersecurity certification for information and telecommunications goods and services that firms seek to provide in the EU, which is regulated by the ENISA[104]. Since 2018, the Cyber Diplomacy Toolbox is a European political kit to prevent cyberattacks with a tailor-made sanctions regime. The NIS 2 directive applies to this segment as well[105].

The third segment is the technology legislation, which shapes the software and hardware allowed in the internal market. The 2021 Artificial Intelligence Act (AI Act) establishes a risk-assessment mechanism to limit entry to the European market based on a company's AI technologies' risk category[106]. The 2022 EU Chips Act aims to make semiconductor research coherent at the European level, as well as enable a joint effort for rebuilding production capacities and preventing semiconductor production from outsourcing[107]. The EU toolbox for 5G security, aimed to ensure the safe provision, delivery, and functioning of 5G equipment, also falls ins this category[108].

The fourth segment shapes the protection of data itself. This category includes the General Data Protection Regulation (GDPR)[109] and the Data Governance Act (DGA)[110], which govern and ensure the safe and fair use of data. This legislation, which includes the principle of conditionality, became a highly efficient regulatory framework that assures compliance outside a single market without being legally binding.

On the one hand, these four divisions work together to harmonise the internal digital market while increasing its competitiveness, making connections within the market more robust, and deepening the integration tendencies. This policy has already tremendously advanced European people's data independence while enhancing cybersecurity protection, thereby significantly contributing to protecting European digital sovereignty.

[104] European Commission (2019).

[105] European Commission (2020a). 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient'. Press Release.

[106] European Commission (2021). 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final'.

[107] European Commission (2022b). 'Proposal for a regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act). COM/2022/46 final'.

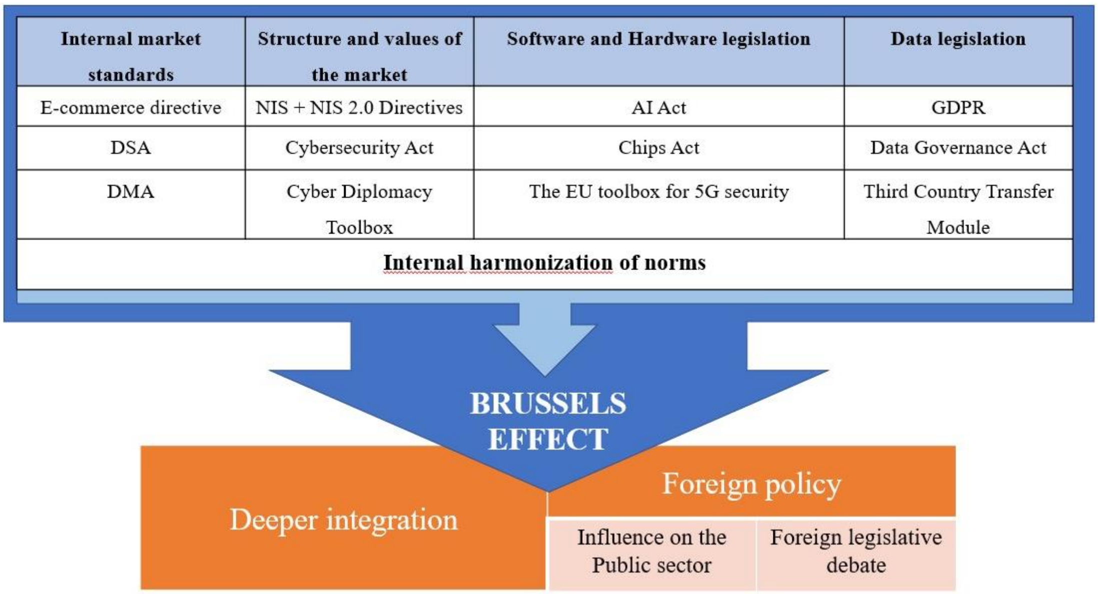
[108] European Commission (2022a). 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Secure 5G deployment in the EU - Implementing the EU toolbox. COM/2020/50 final'.

[109] European Commission (2016).

[110] European Commission (2022i). 'Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)'. Official Journal of the European Union.

On the other hand, as soon as the EU digital market is one of the largest in the world, private firms like Meta and Microsoft must adhere to standards to avoid losing a significant portion of global revenue. Here Brussels Effect caused a spill-over, extending influence beyond the private sector and shaping foreign legislative discussions. The tendency is the following: as soon as tech-giants have no choice but to comply with high EU standards to enter the market, they call for national laws that converge with EU ones to increase legal certainty and interoperability further. An example might be a joint call by key industry players such as Apple, Meta, and Microsoft for a federal law similar to the GDPR, that triggered the US legislative debate on federal privacy law[111].

TABLE III. "BRUSSELS EFFECT"[112]



Internal market standards	Structure and values of the market	Software and Hardware legislation	Data legislation
E-commerce directive	NIS + NIS 2.0 Directives	AI Act	GDPR
DSA	Cybersecurity Act	Chips Act	Data Governance Act
DMA	Cyber Diplomacy Toolbox	The EU toolbox for 5G security	Third Country Transfer Module
Internal harmonization of norms			

The European Union hopes to build on the development made in recent years to become the effective worldwide cyber authority it promises to be in the future. In the end, Europe's experiences with cybersecurity and cyber governance cannot be summarised in any other way than cautious. Only a few subjects are as diverse and adaptable as cyber concerns. Compared to other global cyber players, the European Union stands out. It happens because of its role as an advising governance institution and the gradualism resulting from the necessity to achieve consistency among its members. When confronted with dramatic alteration of the issue at hand (for example, in the shape of innovative

[111] Petkova, B. (2017). 'Domesticating the 'foreign' in making transatlantic data privacy law'. International Journal of Constitutional Law, vol.15 no.4, pp.1135–1156.

[112] Adapted from: Bendiek, A., Stürzer, I. (2022).

evolutions of artificial intelligence or unforeseen manifestations of the Internet of Things), the EU may suffer in a manner that more naturally cohesive political bodies may not. Even if gradualism ends up helping Europe because it leads to careful policy changes, it seems that the EU's approach may fail to address emerging threats in the future.

The EU has developed a forerunner approach for the digital market and should keep and advance its multi-sectoral modus operandi. The "Brussels Effect" may be crucially effective as a soft power mechanism to promote European values and strengthen the voice of the Union as a pioneer in cybersphere governance.

Chapter IV: EU-Russia cybersphere relations

The evolution of EU-Russian ties in the cyber domain has a pervasive history, and its progression may be analysed through a variety of time periods, each representing these interactions in general. They are being carried out on the level of state-to-state relations, as well as bilaterally and supranationally, through international organisations. According to the outcomes of the prior research, it is abundantly evident that there are specific overlapping concerns on the cyber agendas of both players in preventing cyber terrorism and cybercrime. However, over the previous ten years, news releases issued by both Europe and Russia have been rife with charges of hostile cyber activities, which has a negative impact on their relationship. Even the collaboration on the development of cyber standards, which both parties seek, has become stagnant due to the absence of clear guidelines and rules execution. This chapter aims to provide decision-makers with a comprehensive picture of potential future outcomes based on the present outcomes and circumstances. All of these issues will be elaborated on, and the chapter will conclude with the application of the prisoners' dilemma to the pattern of relations between the EU and Russia.

4.1. Periodisation of EU-Russia relations

Cybersphere and cybersecurity have been on the EU-Russian agenda for a while. Currently, it is addressed at the EU-Russia member state bilateral level or multilateral level through the Organisation for Security and Cooperation in Europe (OSCE) and the United Nations. Until 2022 cybersecurity was also included in the Council of Europe (CoE) agenda. However, after the breakout of the war in Ukraine, Russia was suspended from membership.

The development of these relations evolved through the same pattern of periodisation as in EU-Russian overall ties. The first period, from the beginning of the 2000s to the mid-2010s (before the war in Georgia in 2008 and the annexation of Crimea in 2014), reflects general hope for deepening cooperation. During the first period, Moscow and Brussels launched the EU-Russian Road Map for the

Common Space on Freedom, Security, and Justice, which was not solely designed for the cybersphere[113]. However, it touched cyber-associated fields, including fighting against transnational organised crime and terrorism. This cooperation was supposed to be reinforced in the successor agreement of the Partnership and Cooperation Agreement (PCA)[114]. The EU and Russian Federation had an intention to exchange information in the sphere of cyber legislation for tackling virus programs.

Since 2014, Russia has lost EU trust and became seen through a security threat lens. This is particularly true for post-eastern bloc countries, such as Poland, Latvia, Lithuania, and Estonia. The government of Russia or parties associated with it were arraigned by Estonia, Germany, the Netherlands, and Spain for interfering in domestic affairs and espionage[115]. Moscow has denied cyberattacks, reasoning growing concerns as Russophobia and propaganda. In the EU's 2017 cybersecurity reform, Russia is included as one of the threats. To address this threat, the EU strengthened the protection of its institutions, bodies, and agencies through a permanent Computer Emergency Response Team and adopted stricter certification requirements. EU member states also developed a "Cyber Diplomacy Toolbox"[116], including sanctions.

Since the beginning of the second period in 2014, when the Crimean crisis caused misunderstanding and suspended contacts, the EU and Russia rolled back any cooperation in cyberspace. However, these international actors could effectively fight together against multiple common threats in the cybersphere. Areas of cyber terrorism and crime remain two issues of mutual interest and potential beneficial cooperation. After the beginning of the war in Ukraine in 2022, whether EU-Russian cyber cooperation can be rebuilt remains a puzzle. Still, the cybersphere could neither be an area of cooperation nor trigger deepening and expanding relations in other sectors. Today, the EU and Russia see each other as a

[113] Russian Federation (2005). 'Road Map on the Common Space of Freedom, Security and Justice'.

[114] Hernández i Sagrera, R., Potemkina, O. (2013). 'Russia and the common space on freedom, security and justice', CEPS Paper in Liberty and Security in Europe.

[115] Brattberg, E., Maurer, T. (2018). 'Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks', Carnegie Endowment for International Peace.

[116] European Commission. (2020).

threat in cyberspace: the former is afraid of cyberattacks and disruption risks, and the latter is scared of contradicting information and a threat to state stability.

4.2 Factors of the EU-Russia cooperation

Most of the literature covering EU-Russian relations in the sphere of cybersecurity claim Russia's pre-eminence of European cyber potential and the importance of cyber infrastructure and resources in hybrid operations against the West, including the EU[117]. Another research topic is cyber governance and the application of international law to the cybersphere. Some countries' unwillingness to negotiate and adopt legislation in this area causes a stalemate situation, allowing "little green bytes" to move globally, causing damage equivalent to conventional weapons[118]. Another widely-discussed topic is the non-state actors' participation in concealing an unlawful act of a government[119]. Most scholars note that the EU-wide consolidation against cyber threats might be a reaction to Russia's activities. However, the legislation process might be complicated by the legislation procedure barriers and the divide among some member states with closer ties with Kremlin[120].

From an international relations view, the emerging policy field of cyber issues was addressed by the EU as a merely technical issue; however, this sphere little by little became an external aspect of the EU policy and then became a part of the foreign policy topic[121].

The EU sees challenges of cyberspace in both civilian and military security. Accepting the interconnected nature of the Internet and vulnerabilities of open systems, the EU tries a multilateral approach as no single actor can assess and respond to cyber threats on its own. Brussels has exercised this approach across

[117] Limnell, J. (2018). 'Russian cyber activities in the EU', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 65–75.
[118] See above.
[119] Soldatov, A., Borogan, I. (2018). 'Russia's approach to cyber: the best defence is a good offence', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 15–25.
[120] Barrinha, A., Renard, T. (2017).
[121] Rehrl, J. (2018). 'Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union', Luxembourg: Luxembourg Publications Office of the European Union.

several platforms, including the UN GGE and the OSCE[122]. One can see these international bodies as an existing common ground for EU-Russian cyber concert.

4.2.1 Cooperation against cyber terrorism

One of the traditional spheres of bilateral relations of the EU member states and Russia is counter-terrorism, where lies a significant potential for EU-Russia cyber cooperation[123]. In January 2014, when the last EU-Russia summit was held, the parties agreed and adopted a Joint EU-Russia statement on combating terrorism[124]. In this document, participants shared mutual concern on the growing danger of the Internet that can facilitate the expansion of terrorist mindset and create a technological channel of terrorist recruiting among Russian and EU citizens. This statement greeted cooperation to tackle these risks, as well as the possible inclusion of Russia in the "check the web" initiative of the European Police Office (Europol) to monitor terrorist websites.

After 2014, EU-Russian regular consultations on counter-terrorism were put on hold. However, informal discussions to prevent radicalisation were continued between the Russian Ministry of Foreign Affairs (MFA) and the EEAS. There are not many details from scarce press releases and announcements; therefore, we can only guess that cyber issues were on the agenda as an integral part of modern international relations[125,126].

4.2.2 Cooperation against cybercrime

During the first period of EU-Russian relations, both parties were ambitious about expanding relations to prevent cybercrime. An Operational Agreement was prepared by Europol and the Ministry for Internal Affairs of Russia to exchange information on viruses used for criminal purposes; however, it was never implemented[127].

[122] Christou, G. (2016). 'Cybersecurity in the European Union: Resilience, Adaptability and Governance Policy', London: Palgrave Macmillan.

[123] Hernández i Sagrera, R., Potemkina, O. (2013).

[124] Council of the European Union (2014). 'Joint EU-Russia statement on combatting terrorism'.

[125] European External Action Service (2018). 'EU and Russia to hold informal consultations on counter-terrorism in Brussels'.

[126] MFA of Russian Federation (2018b). 'Press release on Deputy Foreign Minister Oleg Syromolotov's meeting with EU Ambassador to Russia Markus Ederer'.

[127] Hernández i Sagrera, R., Potemkina, O. (2013).

The issue that supplements the block in partnership dates back to 2001. That year the Budapest Convention on Cybercrime was signed by Council of Europe's countries and several other states, but Russia abstained. This Convention is the only binding international legal basis for tackling cybercrime. Article 32b was the main stumbling block, as it gives transborder access to computer data for the officials of signatories. Based on the value of mutual assistance, the operation does not require a request, which is inappropriate for Russian authorities and is seen as a possibility to interfere in the state's internal affairs. Even though the Cybercrime Convention Committee highlighted the limited potential of Article 32b in 2014, Moscow remained steadfast[128].

Russia proposed the substitute document in 2017 in the so-called Convention on Cooperation in Combating Cybercrime[129]. There are two differences between the Budapest Convention. First, Convention does not allow trans-border operations without the consent of the state that store the data within its territory. Secondly, it covers more recent cyber threats after 2001 (botnets, spam, etc.)[130]. Russia was looking for international support and was hoping for success, as the approach of the document tried to satisfy both Western and non-Western countries and, as a result, would be global and efficient. In 2018, when the UN General Assembly requested countries' opinions on the issues of the criminal use of information and communications technologies[131], Russia hoped that a wide range of criticism would depict the Budapest Convention as insufficient and clear the necessity for a new "legal umbrella" to be developed[132]. Even though EU member states did not support this resolution, some of them sent their reports to the Secretary-General. Unlike the expectations of Moscow, they stated the effectiveness of the Budapest Convention and that the mechanism in it should be expanded rather than replaced. For instance, Germany claimed that the Convention on Cybercrime is well applicable to tackle ongoing cybercrime issues effectively:

[128] Council of Europe (2014). 'T-CY Guidance Note # 3 Transborder access to data (Article 32)'.

[129] UNGA (2017).

[130] Chernenko, E. (2017). 'The virtual clash of super powers', Kommersant.

[131]UNGA (2018b). 'Resolution A/RES/73/187: countering the use of information and communications technologies for criminal purposes'.

[132] MFA of Russian Federation (2018c). 'Press release on the UN General Assembly adoption of a Russian-proposed resolution on combating cyber crime'.

"In this connection, the Convention has proved to be an appropriate tool to combat cybercrime, which is also open to third countries"[133]. The approach of Western states was always to preserve the Budapest Convention and reform it through integrating new members and updating mechanisms[134]. To keep the Budapest Convention up to date, its Committee issued guidance notes, including botnets, spam, and other offences, which Russia included in an alternative document. However, Russia has not changed its view on the Convention.

As a result, in terms of cybercrime prevention, EU-Russia cooperation is stuck in inconsistency and lack of ability to find a compromise. From a technical point of view, there is no mutual legal basis for such cooperation, neither between Russian authorities and Europol or Eurojust nor on the ground of existing documents. The EU is not interested in developing an alternative to the Budapest Convention approaches. The partnership between Russia and the EU in this area is insufficient.

4.2.3 Cyber operations

One of the major controversial and slow-burning topics in EU-Russian relations is cyber operations to interfere with the internal affairs of another country. Some EU member states suffered from attacks from Russian territory or were supposedly organised by the Russian authorities. Taking into account the difficulty of tracking the origins of attacks, Russia claims proofs are insufficient and denies all accusations. All sectors of business, politics and communication activities attribute every other operation to Russia[135]. Cases that are connected with Russia can be grouped into three categories.

The first and most common motive for a disruptive cyber action is the manipulation of public opinion and tit for tat response to anti-Russian policies. In the spring of 2007, Estonia became a place of the most well-known EU-Russia cyber case, which some scholars call the "Bronze Soldier crisis". The decision of

[133] UNGA (2019a). 'Countering the use of information and communications technologies for criminal purposes: report of the secretary-general'.

[134] Hakmeh, J. (2018). 'Cyberattack revelations appear to undercut Russia's UN efforts', Chatham House.

[135] Herpig, S., Reinhold, T. (2018). 'Spotting the bear: credible attribution and Russian operations in cyber- space', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 33–43.

Tallinn municipal authorities to remove the bronze statue of the soviet soldier from a city centre had a negative response from the Russian-speaking population, causing protests that led to violence and the death of one person. Simultaneously, many governmental, media, and bank websites stopped working under attack. Firstly, the cyberattacks were amateur and undeveloped, such as denial of service (DoS) and distributed denial of service (DDoS) attacks, rounds of junk mail spreading, and automatic bot commenting. Nevertheless, at some point, attacks spilt over on critical information infrastructure of Estonia, including domain name servers (DNS), international routers, and the network nodes of telecommunications companies[136]. The result was most disturbing, rather than damaging, as it caused inconvenience in accessing targeted web pages. Tallinn accused the Kremlin of the attack: Foreign Minister of Estonia Urmas Paet blamed the Russian government for organising cyberattacks, interpreting them as a threat "against the whole European Union"[137]. That case triggered the inclusion of cybersecurity in the global challenges and critical threats of the Report on the Implementation of the European Security Strategy in 2008[138]. Moscow denied any accusations. In Autumn 2007, the Estonian Defence Minister Jaak Aaviksoo accepted that there was "not sufficient evidence of a Russian governmental involvement"[139]. Afterwards, it turned out that the attack was run by the pro-Kremlin youth movement "Nashi", and even one of its activists confirmed this[140].

One more example of disruptive cyber interference relates to Spain. In autumn 2017, the spokesperson Íñigo Méndez de Vigo and Defence Minister María Dolores de Cospedal stated that Russian hackers were interfering in the Catalonian crisis. Officials tried to talk carefully about the attacks and were not blaming Kremlin directly, saying that the flow of fake news originated "from Russian territory". However, Spanish media accused the Russian "troll factory" – the Internet Research Agency. Simultaneously, the Foreign Minister of Spain, Alfonso Dastis, said there were "fairly well-corroborated reports" that Russian hackers were

[136] Pernik, P. (2018). 'The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 33–65.
[137] BBC News (2007). 'Russia accused of “attack on EU”'.
[138] Council of the European Union (2008). 'Report on the Implementation of the European Security Strategy'.
[139] Blomfield, A. (2007). 'Russia accused over Estonian 'cyber-terrorism'', The Telegraph.
[140] Lowe, C., 2009, 'Kremlin loyalist says launched Estonia cyber-attack', Reuters.

organising attacks to "destabilise" the EU. The reasoning of the Foreign Minister was based on the Russian interest in causing discord between members of the EU, assuming that the "country does not feel comfortable with the unity of the European project"[141]. Russian Minister of Foreign Affairs Sergey Lavrov denied any interference and classified these accusations as an example of the "anti-Russian hysteria", as well as the inability of the West to deal with their internal problems[142].

The second category is interference in elections. Some experts believe that Kremlin influenced "Macron leaks" during the 2017 French presidential campaign. The team of then-candidate Emmanuel Macron was hacked, and thousands of internal emails and other documents were stolen and released right before the second round. The attack was aimed to discredit "the most anti-Russian, pro-NATO and pro-European Union candidate in the presidential race"[143]. According to experts, an orchestrated fake news campaign occurred before the leaks, including rumours and forged documents[144]. There was no clear evidence of the Russian governmental trail; Russian authorities denied any connection again. The Kremlin spokesman, Dmitry Peskov, stated that Russian cyber involvement targeting the French election was "completely incorrect"[145].

The third type of interference is cyber espionage. Since 2015, Foreign and Defence ministries, political parties, media, and business companies from the EU have become victims of a number of sophisticated attacks, which caused hackers to access confidential data. Hans-Georg Maassen, President of the Federal Office for the Protection of the Constitution of Germany, directly accused Russia of such attacks against his country. According to the official, Russia was "bolstering cyberattacks, propaganda, and other efforts to destabilise German society". Kremlin refused any accusations[146]. Dmitry Peskov said that "Russia was blamed for almost every attack in the world without a tangible proof"[147].

[141] Diez, A. (2017). 'Government confirms intervention of Russian hackers in Catalan crisis', El Pais.

[142] Ara.cat (2017). 'Russia denies meddling in Catalonia, attributes accusations to 'hysteria' of Spanish government'.

[143] Nossiter, A., Sanger, D. (2017). 'Hackers Came, but the French Were Prepared', The New York Times.

[144] Vilmer, J.-B. (2018). 'Lessons from the Macron Leaks', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 75–85.

[145] Deutsche Welle (2017). 'Suspected Russia hackers 'targeted Macron campaign''.

[146] Shalal, A. (2017). 'Germany challenges Russia over alleged cyberattacks', Reuters.

[147] Nikolskaya, P. (2018). 'Kremlin dismisses allegation Russia behind German cyber attack', Reuters.

In 2018, four Russians were accused of hacking the headquarters of the Organisation for the Prohibition of Chemical Weapons (OPCW), based in the Hague, the Netherlands. Authorities noted that four men with diplomatic status were working for the Russian intelligence office (GRU). They tried to commit a cyberattack against the OPCW servers remotely. However, when that attack was not successful, they tried to organise another attack on Wi-Fi networks in place in The Hague. According to Dutch officials, the reason for the attack was to disrupt OPCW and the Skripal poisoning investigation. The attack failed with the assistance of officials from the United Kingdom, and these four hackers were expelled[148]. EU officials condemned Russia for "undermining international law and institutions"[149]. Once again, the Ministry of Foreign Affairs of the Russian Federation denied the accusations as an "anti-Russian spy mania campaign" and "staged propaganda"[150].

The issue of "alleged" Russian cyber involvement and disinformation campaigns remains problematic and disputable. In 2015, the European Council made a decision to launch the Strategic Communication Task Force (StratCom) as a part of the EEAS to "challenge Russia's ongoing disinformation campaigns". In 2016, the European Parliament adopted a resolution that accused Kremlin of "challenging democratic values, dividing Europe and gathering domestic support, and creating the perception of failed states in the EU's Eastern neighbourhood", "weakening EU cooperation and the sovereignty, political independence and territorial integrity of the Union and its member states"[151]. The same year, the Joint Framework on countering hybrid threats was supported by the European Commission. In 2018, it was followed by the Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats[152]. In the second part

[148] Crerar, P., Henley, J., Wintour, P. (2018). 'Russia accused of cyber-attack on chemical weapons watch- dog', The Guardian.

[149] European Commission (2018c). 'Joint statement by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and High Representative/Vice- President Federica Mogherini'. Press release.

[150] MFA of Russian Federation (2018a). 'Comment by the Information and Press Department on the accusations against Russia by the Dutch defence ministry'.

[151] European Parliament (2016). 'Resolution on EU strategic communication to counteract propaganda against it by third parties'.

[152] European Commission (2018a). 'A Europe that Protects: The EU steps up action against dis- information'. Press release.

of the same year, to prepare for and strengthen the resilience of the 2019-2020 elections, EU leaders decided to boost their cyber defence. Member state officials suggested an Action Plan on Disinformation, which included four spheres: 1) improved detection, 2) coordinated response, 3) online platforms and industry, and 4) raising awareness and empowering citizens[153]. Even though the widespread cyberattack cases did not during the 2019 elections, it is challenging to justify whether this resulted from those efforts.

The latest accusation happened in 2021 in Ireland, during the COVID-19 pandemic. Russia denied its involvement and offer its support in the investigation[154].

However, it is worth noting that some EU countries have started to cooperate with Russia on cyberattack prevention on a bilateral basis. France, Germany, and Spain were holding talks with Russia. French officials are particularly active. Two meetings in 2018 and 2019 of Presidents Emmanuel Macron and Vladimir Putin led to a "regular dialogue" on cyber issues between the two countries. Several high-level inter-agency meetings followed. The French Digital Ambassador Henri Verdier evaluated this dialogue as "letting countries better understand each other, create communication channels and incident reaction mechanisms".

4.3 Standardisation of norms and confidence-boosting measures

Notwithstanding the Crimea crisis and allegations of cyberattacks, EU member states did not stop cooperation with Russia on the cyber agenda on regional and global multilateral levels. In 2013, within OSCE, participants adopted confidence-building measures (CBMs) to mitigate the threat of using information and communication technologies in conflicts. Fifty-seven member countries created formal communication channels to avoid potential conflicts caused by cyber operations and encouraged information exchange on their cyber policies and projects. In 2016, the OSCE expanded the CBM list. Members of the organisation reassured their wish to continue deepening and broadening information exchange

[153] European Commission (2018b). 'Action plan on disinformation: commission contribution to the European Council'.
[154] MFA of Russian Federation (2021). 'Comment by Press Secretary of the Russian Embassy in Ireland on the Cyber Attack on the healthcare system of Ireland "Health Service Executive" (HSE) on May 14, 2021'.

at the official and expert levels to decrease the risks of crises and confrontation. Participants showed a willingness to share and discuss cybersecurity practices stemming from using ICTs and encouraged ICT vulnerabilities reporting[155]. The OSCE has not yet provided the official effectiveness evaluation of these solutions.

The UN remains the central multilateral platform for developing CBMs and behaviour norms in cyberspace. The UN GGE reported a consensus on "promoting a peaceful, secure, open and cooperative ICT environment" in 2013. The report began proclaiming that "measures that could enhance stability and security include norms, rules and principles of responsible behaviour of states, voluntary measures to increase transparency, confidence, and trust among states and capacity-building measures". It was the first time when the report highlighted two principles that are the most disputable among experts today: the application of international law norms in the cybersphere and, at the same time, state sovereignty to state conduct of ICT-related activities and states jurisdiction over ICT infrastructure within their territory[156].

In 2015, the UN GGE presented an updated consensus report, that created the cornerstone for a globally recognised cyber code of conduct. The paper included 11 principal norms, such as a determination that states should not consciously permit their territory to be used for the purposes of cybercrime, should not consciously enable ICT operations that harm critical infrastructure, and should take action to stop the proliferation of malicious technologies and the use of harmful hidden functions[157]. However, members failed to reach an agreement when the GGE met again in 2017. The stumbling block for the 25 countries was applying the right to self-defence, as a part of international humanitarian law, to cyber operations[158]. Western countries agreed that if the UN Charter's right to self-defence is included, it should also be applied to cyberspace. Russia was hesitant and unready to put this down on paper. Even though the initiative failed, which influenced the

[155] Organisation for Security and Cooperation in Europe (2016). 'Decision No. 1202. OSCE confidence- building measures to reduce the risks of conflict stemming from the use of information and com- munication technologies'.
[156] UNGA (2013). 'Resolution A/68/98: report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security'.
[157] UNGA (2015b). 'Resolution A/70/174: report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security'.
[158] Väljataga, A. (2017). 'Back to square one? The fifth UN GGE fails to submit a conclusive report at the UN general assembly', CCDCOE.

intensity of the UN GGE operation, in December 2018, the United States drafted a resolution at the UN GA, which called for a new session of the Group. The United States intentions were:

> *"[…] to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of states, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by states".*
>
> *UN General Assembly, 2018*[159]

In April 2019, for example, the Charter of Trust partners met to discuss the latest developments around the EU Cybersecurity Act. Most EU member states supported the document, which was approved by a substantial majority of votes. Russia voted against, as it had already put its proposal for the 2015 Code of conduct on the table, which did not find support from Western states.

Russia, as a response, called for establishing an open-ended working group (OEWG) to elaborate rules, norms, and principles for appropriate cyber behaviour. The working group would, among other things, examine present and future risks, as well as potential countermeasures[160]. This document was promoted by members of BRICS, the Shanghai Cooperation Organisation (SCO), and the Collective Security Treaty Organisation (CSTO). The resolution was adopted by the UN GA by a majority of votes too, even though EU states voted against it. It was unidentified whether or not two bodies would interact and if it would be possible to cooperate in such a format instead of competing, even though texts do not have any significant differences. However, when the GGE and the OEWG started functioning, Russia continued to participate in the work of the GGE, while many EU members participated in the OEWG format.

[159] UNGA (2018a). 'Resolution A/C.1/73/L.37: advancing responsible state behaviour in cyberspace in the context of international security'.

[160] UNGA (2018c). 'Resolution A/RES/73/27: developments in the field of information and telecommunications in the context of international security'.

In 2021, under the GGE format, Russia and some EU member states reaffirmed norms of behaviour in cyberspace in the context of international security, including the prohibition of hacking another state's critical infrastructure in peacetime or sheltering cyber criminals.

In the end, it is doubtful that such a bipolar approach will lead to a universal legally-binding document on cyberspace. The adoption of two similar resolutions was meant to create two UN mechanisms for two approaches, predictably based on bipolar sets of values, so the development of CBMs and norms in cyberspace would de-facto lead to stalemate and stagnate the process of adoption in the end. Mutual participation in both formats could create positive momentum for EU-Russia relations. However, much will be determined by the relationships between the United States, Russia and China as well as the relations between the United States and the EU.

4.4 Application of the prisoner's dilemma to the case study of EU-Russia bilateral relations

When analysing the normative acts of Russia and the European Union, one can conclude that the interests of states can be mutually beneficially represented. This statement allows proceeding with the application of the prisoner's dilemma. The summary of this subchapter is presented in the matrix in Table IV.

First of all, cooperation between the EU and Russia is possible only on the acceptance of investigation results of past offensive cyber operations and the deterrence of future cyberattacks. According to the scenario, cooperation will first happen in two overlapping areas: countering terrorism and fighting against transnational organised crime. The coverage of these areas in the legal field of the two actors does not contradict each other and therefore creates fertile ground for the development of cooperation. Creating a mutual legal basis for such cooperation between Russia (Roskomnadzor, FSB) and European authorities (ENISA, Europol) will strengthen bilateral cyber resilience and bring more security globally, reflecting the transborder nature of the cybersphere.

TABLE IV. EU-RUSSIA CYBER PRISONER'S DILEMMA

		The European Union (A)	
		Cooperates (+)	Does not cooperate (-)
Russian Federation (B)	Cooperates (+)	A+B+: Highly unlikely scenario • Past cyberattacks are investigated, future hacks are deterred; • Joint effort of countering terrorism and fighting against transnational organized crime; • Governance exchange: Brussels Effect; • Exchange within private and public sectors of both actors; • Cyber R&D cooperation; • ICT development; • Increase of ICT trade flows; • Cooperation on the development of international norms and principles of cyberspace.	A-B+: Highly unlikely scenario For EU: • Uses information governance tools from Russia as a case study; • Advance protocols for identifying and preventing proxy attacks; • Adoption of European norms and values for global cyber governance in the UN. For Russia: • Cutting of ITC goods flows of EU; • Sanctions against Russia.
	Does not cooperate (-)	A+B-: Unlikely Scenario: For EU: • Intellectual rights violation; • Continuation of cyberattacks, sabotage of EU cyber infrastructure; • EU attracts IT specialists. For Russia: • Usage of the European Intellectual Property; • Safe infrastructure; • Brain Drain from Russia; • Adoption of norms of state information sovereignty in the UN.	A-B-: Highly likely scenario • Cyber confrontation; • Escalation of cyberattacks; • R&D and business relations suspended; • Bilateral sanctions; • Stumbling block on the development of international cyber norms.

The legislation and administrative structure for cybersecurity in the EU are more developed than in Russia: the law regulates, among other things, 5G, AI, cloud data, etc. The draft cyber strategy of the Russian Federation states that one of the directions of the state's activities to ensure cybersecurity is the "systematic improvement of the legislation of the Russian Federation in the field of cybersecurity, including through the adaptation of legal norms from the laws of foreign states". Thus, the Brussels Effect can also work for Russia, spreading the developed legislation systems as a good practice.

Another area of positive interaction could be formalising knowledge exchange between institutions, security authorities, academia, and industry. For example, it might be the creation of situational centres and involving the expert community to exchange information on measures and means to ensure cybersecurity. Mutual staff training will help improve not only the skills of specialists but also establish personal relationships, simplifying the interaction between the bodies and organising more streamlined cooperation. Such interaction can take place both at the level of public services and at the level of educational and non-profit organisations.

Furthermore, economic policy and technological skills should be explicitly included. Public institutions, businesses, the scientific community, and civil society must cooperate in a much more coordinated way at the inter-EU-Russia level than they do it today. This kind of interaction can establish the foundation for democratic, economic, and technical conditions and strengthen the necessary infrastructure, know-how, and advanced technology exchange channels.

Diplomacy must complement technical and technocratic efforts. Standardisation of international norms is crucial for trust and security in the cyber and information space both for Russia and the EU. Actors should continue working in this sphere through bilateral relations and on the UN level through the GGE and OEWG.

In case when at least one of the actors decides not to cooperate, the quality and the level of benefit of cooperation significantly drops, causing zero-sum results. If the European Union cooperates, while Russia's response is negative, the Union might suffer from the continuation of cyberattacks. The Concept of cybersecurity in Russia states that the country will support local producers in implementing and using software and hardware, including cybersecurity tools, instead of foreign analogues. For bilateral relations, it may mean the duplication of European cyber services in Russia, which may lead to disputes regarding intellectual rights violations. Russia would enjoy the benefits of one-sided cooperation in using European know-how while keeping its infrastructure safe. In this scenario, Russia can also use a compromise from European partners to build a coalition on the supranational UN level to promote its vision of cyberspace. However, it is important to highlight that the openness and opportunities of the European market may attract professionals to move from Russia to the EU.

In the opposite scenario, when Russia cooperates and the EU does not, the EU might benefit from using information governance tools to improve its data management systems and advance protocols for identifying and preventing proxy attacks. As an alternative to the previous scenario, the compromise from Russia may lead to adopting European norms and values for global cyber governance, which may be seen as a victory of the Western approach in the cyber domain. It is worth mentioning that China will not welcome such an outcome. The brain drain from Russia is less possible, as the European market will probably be closed for Russian professionals. For Russia, such a scenario will mean the inability to use ITC goods from Europe.

The worst-case scenario, when both actors implement a hostile policy against each other, may lead to cyber confrontation and public and private relations shut down. In case of offensive attacks coming from both sides, the infrastructure of the EU and Russia may be significantly damaged. As a response to the attacks, actors may adopt sanctions against each other that will badly influence the economic situation both in Russia and Europe. In the international arena, this scenario may lead to a stumbling block to the development of cyber norms and governance, which will cause the incapability of global systems to follow the developments of ITC use for offensive purposes.

Unlike the original prisoner's dilemma (when the prisoner, who cooperates, gets worse punishment than the other one who does not), the worst outcome for both players is seen in the case of mutual non-cooperation. This situation brings negative consequences for the global community and not only for the two actors in focus. Moreover, the negative sum of the scenario causes damage and disadvantages for both parties.

Conclusion

This thesis aims to examine the possible consequences of EU-Russia relations in the cybersphere, considering the prisoner's dilemma model of the decision-making. Understanding the scenarios of the development of EU-Russia bilateral relations is valuable both for politicians and scholars of these actors as well as the international community, because the evolution of affairs of these strong superpowers in such a tangible and interconnected cyber domain may affect the whole world. The research suggests that there are no significant contradictions between Russia and the EU in domestic and strategic legislation; therefore, both cooperation and clashes are possible. The outcome is based on the decision-making, the desire of actors to fulfil their self-interest, and the ability to reach compromises.

The paper gives four possible scenarios: two with a zero-sum, one with a negative-sum, and one with positive-sum outcomes. However, putting the results in the context of the current and past events, taking into consideration the high level of democracy in the Union and the irreplaceability of the Russian decision-making elite, one may observe a more apparent and distinguished possibility to these scenarios.

The conflict in Crimea was a defining moment in EU-Russia relations, and the cybersphere is no exception. The cooperation between the EU and Russia on cyber issues began long before 2014 and has, inescapably, been poorly injured by the outcomes of that events. The ongoing war in Ukraine is worsening and stopping diplomatic interactions and technological exchange. Furthermore, the general "anti-western" narrative of the Russian political elite and the recent dynamics of the relations with the EU make the cooperation scenarios (B+) highly unlikely (therefore, track B- is more possible).

At the same time, considering the conflict in Ukraine, which began in 2022, the European Union will not want to collaborate with the aggressor (therefore, track A- is more possible).

Putin's attack on Ukraine has claimed violence and significant economic loss for Russia and the EU. At an informal summit in Versailles, EU leaders decided to drastically cut imports from Russia and take more actions to enhance European defences. Under such conditions, it is hard to discuss re-establishing economic relationships that did not exist before the conflict. Any subsequent dialogue will require an end to the conflict.

At the same time, even if the war ends, this will not mean that the parties can move on to the usual agenda, as it was before February 2022. The future "peaceful" attitude of the European political elite towards the "irreplaceable" leadership of Russia is unclear. Over the past few years, Russia has spoken to the EU in the language of ultimatums and undermined trust by carrying out cyberattacks. In the event of the restoration of peace, the current government has already lost its credibility. Restoring dialogue between the EU and the Russian Federation will require adherence to democratic rules by the former: namely, the alternation and legitimacy of power through fair elections, to allow the "fresh blood" to influence the decision-making.

Furthermore, considering ongoing disputes between China and the US, the EU and Russia seem to have already decided. Weakened and isolated after the war break-out, Russia will increasingly rely on the Chinese market to offload its supplies, fostering the geopolitical consensus between Moscow and Beijing. In the cybersphere, it may trigger further dependency of Russia on Chinese cyber equipment and software. The EU would not sacrifice its most significant market segment in the US until it establishes its domestic production of cyber devices. That will bring the EU and Russia further away from each other. The longer the EU and Russia will stay distant, the further they will go away toward new political magnetic poles. It may remind us of the iron curtain, that may become digital for the 21st Century, which is primarily damaging to multilateral values and person-to-person connections, that are essential and crucial for global politics.

Even without considering the current geopolitical problems, the interaction of the Russian Federation and the EU in cyberspace, in any case, can lead to clashes. The Brussels Effect concerning the Russian Federation is limited: the contradiction in the two actors' values and existing legislation will hardly allow Russia to absorb the norms adopted in the EU. For example, "the right to be forgotten" is absent in the Russian Federation. However, it contradicts the Russian government's requirement to store users' data in social networks and instant messengers. It is especially true taking into account the existing "opposing West" paradigm in the Russian political narrative.

The sphere of information security and content regulation can become another stumbling block between the Russian Federation and the EU. If Russia closes its RuNet sector from external influence, it will cut off all possible information flow from the EU, putting interaction in this area on hold.

The settlement of the Ukraine conflict remains a major challenge to any future relations development. Re-activation of cyber cooperation would also require Russia to deal with the concerns of EU member states on the proclaimed interference in their internal affairs. Even though the dialogue on cyberspace has taken place on an interstate level, the cooperation between Russia and the EU is being kept to a minimum. Differences in approaches towards sovereignty, norms, and appropriate behaviour limit the possibilities for substantive cooperation, which are another barrier to a compromise. In the current state of EU-Russian relations, little can be done to overcome these difficulties. Therefore, confrontation is more likely, than cooperation.

Nevertheless, even when confrontation is unavoidable, it is still possible to diminish the consequences. For this, Russia and the EU are required to implement multilateral discussions on cyberspace within existing UN formats of GGE and OEWG on topics that are not controversial in actors' policies. These minor steps toward each other might be:

1) establishing a fair exchange of information on cyber threats and attribution (falling under the category of "communication and information exchange" in the GGE context) on the operational and technical level;

2) establishing standard legal practices whether the use of a cyberattack is a legitimate tool within the scope of international law and how and in what form such actions can be used.

In the case of achievement of objects above, information sharing can be expanded, for example, exchange on cyber threats between military branches. It is important to note that this sectoral exchange needs to stay separate from intelligence to achieve better results, as this keeps political considerations. Furthermore, new coordination centres are required, rather than officials working alone and duplicating work in the EU and Russia.

Even though this paper strongly suggests cooperation, the application of deterrence techniques in cyberspace is also possible. Both actors need to invest more in their information systems to make them resilient to any attack and introduce such tools as "denial by the defence" and "entanglement". As a result, regardless cybered conflicts are likely to continue, they will provoke fewer existential consequences.

After all, it is worth mentioning that there is scope for more profound further research. It can be expanded and include data from Russia and the EU on the possible economic impact of cooperation/confrontation in the cybersphere and public opinion polls (on the protection of cyberspace and/or government approval) as additional merit for the discussion-making. Technical expertise from ITC specialists using peer-reviewed empirical research could verify scenario probability. Moreover, the model can be applied to other bilateral cyber relations and can be updated in a timely manner.

It is important to note that the current paper does not seek to predict the upcoming events but rather analyse tendencies and applies them to the decision-making model. The prevalent message taken from the scenarios presented earlier – international cooperation is essential for a secure cybersphere —is helpful for other developed and developing, rich and poor countries, as the World Wide Web overcomes all physical boundaries between countries and evens the playing field in the hierarchy between hegemons and less-powerful states. Taking into account recent cyberattacks worldwide, technologically developed nations were shown to be just as vulnerable to cyber threats as nations in the early stages of cyber development. In addition to extensive technical skillset, the needs for robust cybersecurity in the twenty-first century now involve and necessitate more political action than in the past. Therefore, facing the growing threats and risks in cyberspace, both Russia and the EU have a chance to become closer together and intensify cooperation – even with other conflicts unresolved.

Bibliography

APC (2019). 'UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online'. [online] Available at: https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed [Accessed: 14 June 2022].

Ara.cat (2017). 'Russia denies meddling in Catalonia, attributes accusations to 'hysteria' of Spanish government'. [online] Available at: www.ara.cat/en/Russia-Catalonia-attributes-accusations-Span ish_0_1907209354.html [Accessed: 14 June 2022].

Bangemann Group (1994). 'Report on Europe and the Global Information Society', Bulletin of the European Union, Supplement 2/94. [online] Available at: http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf [Accessed: 14 June 2022].

Barrinha, A., Farrand-Carrapico, H. (2018). 'How Coherent Is EU Cybersecurity Policy?', LSE European Politics and Policy (EUROPP) Blog. [online] Available at: https://blogs.lse.ac.uk/europpblog/2018/01/16/howcoherent-is-eu-cybersecurity-policy/ [Accessed: 14 June 2022].

Barrinha, A., Renard, T. (2017). 'Cyber-diplomacy: the making of an international society in the digital age', Global Affairs, vol.3 no.4-5, pp. 353–364. [online] Available at: www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924?scroll=top&needAccess=true [Accessed: 14 June 2022].

BBC News (2007). 'Russia accused of 'attack on EU''. [online] Available at: http://news.bbc.co.uk/2/hi/europe/6614273.stm [Accessed: 14 June 2022].

BCS Express (2017). 'LinkedIn leaves Russia [LinkedIn уходит из России]'. [online] Available at: https://bcs-express.ru/novosti-i-analitika/linkedin-ukhodit-iz-rossii [Accessed: 14 June 2022].

Bendiek, A., Stürzer, I. (2022). 'Advancing European Internal and External Digital Sovereignty', Stiftung Wissenschaft und Politik. [online] Available at: https://www.swp-berlin.org/en/publication/advancing-european-internal-and-external-digital-sovereignty [Accessed: 14 June 2022].

Bertuzzi, L. (2022). 'China, Russia prepare new push for state-controlled internet'. EURACTIV.com, February 28. [online] Available at: https://www.euractiv.com/section/digital/news/china-russia-prepare-new-push-for-state-controlled-internet/ [Accessed: 14 June 2022].

Biscop, S., Andersson, J. (2008). 'The EU and the European Security Strategy: Forging a Global Europe'. Abingdon: Routledge.

Blomfield, A. (2007). 'Russia accused over Estonian 'cyber-terrorism'', The Telegraph. [online] Available at: www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html [Accessed: 14 June 2022].

Brattberg, E., Maurer, T. (2018). 'Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks', Carnegie Endowment for International Peace. [online] Available at: https://carnegieen dowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber- attacks-pub-76435 [Accessed: 14 June 2022].

Carrapico, H., Barrinha, A. (2017). 'The EU as a Coherent (Cyber) Security Actor?', Journal of Common Market Studies, vol. 55 no.6, pp. 1254–1272.

Cavelty, M.D. (2022). 'Cybersecurity between hypersecuritization and technological routine', in Tikk, E., Kerttunen, M. (eds.) Routledge Handbook of International Cybersecurity. New York: Routledge, pp. 11-21.

Chernenko, E. (2017). 'The virtual clash of super powers', Kommersant. [online] Available at: www.kommersant.ru/doc/3270136 [Accessed: 14 June 2022].

Chernenko, E., Ivanov, M. (2013). 'The concept of cybersecurity has diverged from the state strategy. So far, only public figures and businesses like the senators' proposals [Концепция кибербезопасности разошлась с государственной стратегией. Предложения сенаторов нравятся пока только общественникам и бизнесу]'. Kommersant, November 29, no.220, p. 2. [online] Available at: www.kommersant.ru/doc/2355154 . [Accessed: 14 June 2022].

Christou, G. (2016). 'Cybersecurity in the European Union: Resilience, Adaptability and Governance Policy', London: Palgrave Macmillan.

Correa, H. (2001). 'Game theory as an instrument for the analysis of international relations' 立命館国際研究, vol.14 no.2., pp.187-208. [online] Available at: http://www.ritsumei.ac.jp/ir/isaru/assets/file/journal/14-2_hector.pdf [Accessed: 14 June 2022].

Council of Europe (2014). 'T-CY Guidance Note # 3 Transborder access to data (Article 32)'. [online] Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a [Accessed: 14 June 2022].

Council of the European Union (2008). 'Report on the Implementation of the European Security Strategy'. [online] Available at: www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ reports/104630.pdf [Accessed: 14 June 2022].

Council of the European Union (2014). 'Joint EU-Russia statement on combatting terrorism'. [online] Available at: www.consilium.europa.eu/media/23839/140835.pdf [Accessed: 14 June 2022].

Council of the European Union (2022). 'A Strategic Compass for Security and Defence'. [online] Available at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf [Accessed: 14 June 2022].

Cremona, M. (2008). 'Coherence through Law: What Difference Will the Treaty of Lisbon Make?' Hamburg Review of Social Sciences, vol.3 no.1, pp. 11–36.

Crerar, P., Henley, J., Wintour, P. (2018). 'Russia accused of cyber-attack on chemical weapons watch-dog', The Guardian. [online] Available at: www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body [Accessed: 14 June 2022].

Demchak, C.C. (2012). 'Cybered conflict, cyber power, and security resilience as strategy', in Reveron D. (ed.), Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Washington, DC: Georgetown Press, pp. 121-136.

Deutsche Welle (2017). 'Suspected Russia hackers 'targeted Macron campaign''. [online] Available at: www.dw.com/en/suspected-russia-hackers-targeted-macron-campaign/a-38580848 [Accessed: 14 June 2022].

Diez, A. (2017). 'Government confirms intervention of Russian hackers in Catalan crisis', El Pais. [online] Available at: https://elpais.com/elpais/2017/11/10/inenglish/1510329788_994258.html [Accessed: 14 June 2022].

European Commission (1993). 'Growth, Competitiveness, and Employment. The Challenges and Ways Forward into the 21st Century'. [online] Available at: https://op.europa.eu/en/publication-detail/-/publication/4e6ecfb6-471e-4108-9c7d-90cb1c3096af [Accessed: 14 June 2022].

European Commission (2000). 'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')'. Official Journal of the European Union. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031 [Accessed: 14 June 2022].

European Commission (2013). 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2013:0001:FIN [Accessed: 14 June 2022].

European Commission (2016). 'Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)', Official Journal of the European Union. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504 [Accessed: 14 June 2022].

European Commission (2017). 'State of the Union 2017 – Cybersecurity: Commission Scales up EU's Response to Cyber-Attacks'. [online] Available at: http://europa.eu/rapid/press-release_IP17-3193_en.htm [Accessed: 14 June 2022].

European Commission (2018a). 'A Europe that Protects: The EU steps up action against dis-information'. Press release. [online] Available at: http://europa.eu/rapid/press-release_IP-18-6647_en.htm [Accessed: 14 June 2022].

European Commission (2018b). 'Action plan on disinformation: Commission contribution to the European Council'. [online] Available at: https://ec.europa.eu/commission/publications/action-plan- disinformation-commission-contribution-european-council-13-14-december-2018_en [Accessed: 14 June 2022].

European Commission (2018c). 'Joint statement by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and High Representative/Vice-President Federica Mogherini'. Press release. [online] Available at: http://europa.eu/rapid/press-release_ STATEMENT-18-6026_en.htm [Accessed: 14 June 2022].

European Commission (2019). 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)'. [online] Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj [Accessed: 14 June 2022].

European Commission (2020a). 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient'. Press Release. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 [Accessed: 14 June 2022].

European Commission (2020b). 'Joint Communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade'. [online] Available at: https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:52020JC0018 [Accessed: 14 June 2022].

European Commission (2021). 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final'. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 [Accessed: 14 June 2022].

European Commission (2022a). 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Secure 5G deployment in the EU - Implementing the EU toolbox. COM/2020/50 final'. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:0050:FIN&_sm_au_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ [Accessed: 14 June 2022].

European Commission (2022b). 'Proposal for a regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act). COM/2022/46 final'. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0046 [Accessed: 14 June 2022].

European Commission (2022c). 'Commission invites citizens and organisations to share their views on the European Cyber Resilience Act'. Press release. [online] Available at: https://digital-strategy.ec.europa.eu/en/news/commission-invites-citizens-and-organisations-share-their-views-european-cyber-resilience-act [Accessed: 14 June 2022].

European Commission (2022d). 'Commission welcomes political agreement on new rules on cybersecurity of network and information systems'. Press release. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985 [Accessed: 14 June 2022].

European Commission (2022e). 'Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets'. Press release. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1978 [Accessed: 14 June 2022].

European Commission (2022f). 'Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment'. Press release. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545 [Accessed: 14 June 2022].

European Commission (2022g). 'New rules to boost cybersecurity and information security in EU institutions, bodies, offices and agencies'. Press release. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1866 [Accessed: 14 June 2022].

European Commission (2022h). 'Proposal for a Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2022-2027'. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0030 [Accessed: 14 June 2022].

European Commission (2022i). 'Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)'. Official Journal of the European Union. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868 [Accessed: 14 June 2022].

European External Action Service (2017). 'Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy'. [online] Available at: https://op.europa.eu/en/publication-detail/-/publication/3eaae2cf-9ac5-11e6-868c-01aa75ed71a1 [Accessed: 14 June 2022].

European External Action Service (2018). 'EU and Russia to hold informal consultations on counter-terrorism in Brussels'. [online] Available at: https://eeas.europa.eu/ru/eu-information-russian/39395/eu-and-russia-hold-informal-consultations-counter-terrorism-brussels_en [Accessed: 14 June 2022].

European External Action Service (2022). 'Permanent Structured Cooperation (PESCO) – Factsheet'. [online] Available at: https://www.eeas.europa.eu/eeas/permanent-structured-cooperation-pesco-factsheet-0_en [Accessed: 14 June 2022].

European Parliament (2016). 'Resolution on EU strategic communication to counteract propaganda against it by third parties'. [online] Available at: www.europarl.europa.eu/sides/getDoc.do?pubRef=-// EP//TEXT+TA+P8-TA-2016-0441 + 0+DOC+XML+V0//EN [Accessed: 14 June 2022].

European Parliament and Council of the European Union (2016). 'Directive (EU) 2016/ 1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union'. [online] Available at: http://data.europa.eu/eli/dir/2016/1148/oj [Accessed: 14 June 2022].

Farwell, J., Rohozinski, R. (2012). 'The New Reality of Cyber War', Survival, vol. 54 no.4, pp. 107-120.

Fridman O. (2017). 'The Russian perspective on Information Warfare', Defence Strategic Communications, Vol. 2, pp. 75-76.

Geer, D. et al. (2003). 'Cyberinsecurity: The cost of monopoly'. [online] Available at: http://www.ccianet.org/wp-content/uploads/2003/09/cyberinsecurity%20the%20cost%20of%20monopoly.pdf [accessed 14 June 2022].

Geico, J., 1988, 'Realist Theory and the Problem of International Cooperation: Analysis with an Amended Prisoner's Dilemma Model', The Journal of Politics, vol. 50 no.3, p. 601.

Gerasyukova, M. (2020). 'Restrictions lifted: Roskomnadzor unblocked Telegram [Ограничения сняты: Роскомнадзор разблокировал Telegram]', Gazeta.ru, June 18. [online] Available at: https://www.gazeta.ru/tech/2020/06/18/13122085/unblock.shtml [Accessed: 14 June 2022].

Giles K. (2016). ' Russia's 'New' Tools for Confronting the West'. London: Chatham House, the Royal Institute of International Affairs, pp. 29-31. [online] Available at: https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf . [Accessed: 14 June 2022].

Hakala, J., Melnychuk, J. (2021). 'Russia's strategy in cyberspace'. NATO Strategic Communications Centre of Excellence. [online] Available at: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf . [Accessed: 14 June 2022].

Hakmeh, J. (2018). 'Cyberattack revelations appear to undercut Russia's UN efforts', Chatham House. [online] Available at: www.chathamhouse.org/expert/comment/cyberattack-revelations-appear-undercut-russia-un [Accessed: 14 June 2022].

Hernández i Sagrera, R., Potemkina, O. (2013). 'Russia and the common space on freedom, security and justice', CEPS Paper in Liberty and Security in Europe. [online] Available at: https://ssrn.com/ abstract=2277506 [Accessed: 14 June 2022].

Herpig, S., Reinhold, T. (2018). 'Spotting the bear: credible attribution and Russian operations in cyber-space', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 33–43. [online] Available at: www.iss.europa.eu/sites/default/files/EUISS Files/CP_148.pdf [Accessed: 14 June 2022].

Hunker, J. (2012). 'Policy Challenges in Building Dependability in Global Infrastructures', Computers & Security, no. 21, pp. 705-711.

Kramer, F. (2009). 'Cyberpower and national security: POLICY recommendations for a strategic framework', in Kramer, F., Starr, S., Wentz, L. (eds), Cyberpower and National Security. Dulles: Potomac Books, pp. 3–23.

Kremer, J.-F. and Müller, B., 2013. Cyberspace and International Relations. Heidelberg, : Springer Berlin.

Kukkola J., Ristolainen M. (2018). 'Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders', Journal of Information Warfare, vol. 17 no. 2, pp. 83- 100.

Lake, D. (2013). 'Theory is dead, long live theory: The end of the great debates and the rise of eclecticism in international relations', European Journal of International Relations, vol. 19 no.3, pp. 567-587.

Lawson, S. (2012). 'Putting the 'war' in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States', First Monday, vol.17 no.7, pp. 49-73.

Limnell, J. (2018). 'Russian cyber activities in the EU', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 65–75. [online] Available at: www.iss.europa.eu/sites/default/files/EUISS Files/CP_148.pdf [Accessed: 14 June 2022].

Lindsay, J. R. (2013). 'Stuxnet and the Limits of Cyber Warfare', Security Studies, vol.22 no.3, pp. 365–404.

Lowe, C., 2009, 'Kremlin loyalist says launched Estonia cyber-attack', Reuters. [online] Available at: www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber- attack-idUSTRE52B4D820090313 [Accessed: 14 June 2022].

Maness, R.C., Valeriano, B. (2018). 'International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain', in Brown, C., Eckersley, R. (eds.) 'The Oxford Handbook of International Political Theory'.

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation'. Computer Law and Security Review, vol. 35 no.6, pp. 1-11. [online] Available at: https://pure.uvt.nl/ws/portalfiles/portal/32292292/pdh19_dmvp_The_NIS_Directive_ENISA_s_role_draft_doi.pdf [Accessed: 14 June 2022].

McCarthy, M. (2014). 'The role of games and simulations to teach abstract concept of anarchy, cooperation, and conflict in world politics', Journal of Political Science Education, no.10, pp. 400-413.

MFA of Russian Federation (2018a). 'Comment by the Information and Press Department on the accusations against Russia by the Dutch defence ministry'. [online] Available at: www.mid.ru/en/web/guest/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3367418 [Accessed: 14 June 2022].

MFA of Russian Federation (2018b). 'Press release on Deputy Foreign Minister Oleg Syromolotov's meeting with EU Ambassador to Russia Markus Ederer'. [online] Available at: www.mid.ru/web/guest/evropejskij-souz-es/-/asset_publisher/6OiYovt2s4Yc/content/id/3051634?p_p_id=101_INSTANCE_6OiYovt2s4Yc&_ 101_INSTANCE_6OiYovt2s4Yc_languageId=en_GB [Accessed: 14 June 2022].

MFA of Russian Federation (2018c). 'Press release on the UN General Assembly adoption of a Russian-proposed resolution on combating cyber crime'. [online] Available at: https://mid.ru/ru/foreign_policy/news/1580442/?lang=en [Accessed: 14 June 2022].

MFA of Russian Federation (2018d). 'Foreign Minister Sergey Lavrov's remarks at the 73rd session of the UN General Assembly, New York, September 28, 2018'. [online] Available at: www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/3359296 [Accessed: 14 June 2022].

MFA of Russian Federation (2021). 'Comment by Press Secretary of the Russian Embassy in Ireland on the Cyber Attack on the healthcare system of Ireland "Health Service Executive" (HSE) on May 14, 2021'. [online] Available at: https://mid.ru/ru/detail-material-page/1481117/?lang=en [Accessed: 14 June 2022].

Mueller, M. (2017). 'Will the Internet Fragment? Sovereignty, Globalization and Cyberspace'. London: Polity.

Nikolskaya, P. (2018). 'Kremlin dismisses allegation Russia behind German cyber attack', Reuters. [online] Available at: www.reuters.com/article/us-germany-cyber-russia-kremlin/kremlin-dismisses-allegation-russia-behind-german-cyber-attack-idUSKCN1GE1CI [Accessed: 14 June 2022].

Nossiter, A., Sanger, D. (2017). 'Hackers Came, but the French Were Prepared', The New York Times. [online] Available at: www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html [Accessed: 14 June 2022].

Nuttall, S. (2005). 'Coherence and Consistency', in C. Hill & M. Smith (eds.), International Relations and the European Union, Oxford: Oxford University Press, pp. 91–112.

Nye, J. S. (2010). 'Cyber Power'. Harvard Kennedy School.

Nye, J.S. (2021). 'The End of Cyber-Anarchy?', Foreign Affairs, December 14. [online] Available at: https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy [Accessed: 14 June 2022].

Organisation for Security and Cooperation in Europe (2016). 'Decision No. 1202. OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies'. [online] Available at: www.osce.org/pc/227281?download=true [Accessed: 14 June 2022].

Parker, D. B. (2014). 'Toward a New Framework for Information Security', in S. Bosworth, M. E. Kabay & E. Whyne (eds.), The Computer Security Handbook (6th ed.). New York: Wiley, chapter 3.

Pernik, P. (2018). 'The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 33–65. [online] Available at: www.iss.europa.eu/sites/default/files/EUISS Files/CP_148.pdf [Accessed: 14 June 2022].

Petkova, B. (2017). 'Domesticating the 'foreign' in making transatlantic data privacy law'. International Journal of Constitutional Law, vol.15 no.4, pp.1135–1156. [online] Available at: https://academic.oup.com/icon/article/15/4/1135/4872579 [Accessed: 14 June 2022].

Pomorska, K. & Vanhoonacker, S. (2016). 'Europe as a Global Actor: Searching for a New Strategic Approach', Journal of Common Market Studies, vol.53 no.1, pp. 216–229.

Poundstone, W. (1992). Prisoner's Dilemma. NY: Doubleday, p.8.

Pupillo, L., Griffith, M., Blockmans, S., Renda, A. (2018). 'Strengthening the EU's Cyber Defence Capabilities', CEPS Task Force Report. [online] Available at: https://www.ceps.eu/ceps-publications/strengthening-eus-cyber-defence-capabilities/ [Accessed: 14 June 2022].

Rehrl, J. (2018). 'Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union', Luxembourg: Luxembourg Publications Office of the European Union. [online] Available at: https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1/language-en/format-PDF/source-80572134?fbclid=IwAR2AS5dw8pbwu1OStIg-tMk2immKL-R_0e_ LddMU3ejewHLhCuCV6cAYSSw [Accessed: 14 June 2022].

Romaniuk, S.N. and Manjikian, M. (2021). 'Routledge Companion to Global Cyber-Security Strategy'. London: Routledge.

Romanova, T. and David, M. (2021). 'Routledge Handbook of EU-Russia Relations'. London: Routledge.

Russian Federation (2000). 'Doctrine of Information Security of the Russian Federation', Decree of the President of Russian Federation from 09.09.2000 N PR-1895 (invalid) [Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 г. N Пр-1895) (утратила силу)]. [online] Available at: https://base.garant.ru/182535/ [Accessed: 14 June 2022].

Russian Federation (2005). 'Road Map on the Common Space of Freedom, Security and Justice'. [online] Available at: http://en.kremlin.ru/supplement/3588 [Accessed: 14 June 2022].

Russian Federation (2012a). Federal Law 'On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Regulation of the Activities of Non-Commercial Organizations Acting as Foreign Agents' dated 20.07.2012 N 121-FZ [Федеральный закон 'О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента' от 20.07.2012 N 121-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_132900/ [Accessed: 14 June 2022].

Russian Federation (2012b). Federal Law 'On Amendments to the Federal Law 'On the Protection of Children from Information Harmful to Their Health and Development' and Other Legislative Acts of the Russian Federation' dated 28.07.2012 N 139-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'О защите детей от информации, причиняющей вред их здоровью и развитию' и отдельные законодательные акты Российской Федерации' от 28.07.2012 N 139-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_133282/ [Accessed: 14 June 2022].

Russian Federation (2013a). 'Concept of Cybersecurity Strategy, project'. [online] Available at: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf [Accessed: 14 June 2022].

Russian Federation (2013b). Federal Law On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection' dated 28.12.2013 N 398-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'Об информации, информационных технологиях и о защите информации' от 28.12.2013 N 398-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_156518/ [Accessed: 14 June 2022].

Russian Federation (2014a). Federal Law 'On Amendments to Certain Legislative Acts of the Russian Federation for Clarifying the Procedure for Processing Personal Data in Information and Telecommunication Networks' dated 21.07.2014 N 242-FZ [Федеральный закон 'О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях' от 21.07.2014 N 242-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_165838/ [Accessed: 14 June 2022].

Russian Federation (2014b). Federal Law 'On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection' and Certain Legislative Acts of the Russian Federation on Regulating the Exchange of Information Using Information and Telecommunication Networks' dated 05.05.2014 N 97-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'Об информации, информационных технологиях и о защите информации' и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей' от 05.05.2014 N 97-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_162586/ [Accessed: 14 June 2022].

Russian Federation (2014c). Federal Law 'On Amendments to the Law of the Russian Federation 'On the Mass Media' dated 14.10.2014 N 305-FZ [Федеральный закон 'О внесении изменений в Закон Российской Федерации 'О средствах массовой информации' от 14.10.2014 N 305-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_169740/ [Accessed: 14 June 2022].

Russian Federation (2014d). Federal Law On Amendments to the Certain Federal Law dated 05.05.2014 N128-FZ [Федеральный закон 'О внесении изменений в отдельные законодательные акты Российской Федерации' от 05.05.2014 N 128-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_162575/3d0cac60971a511280cbba229d9b6329c07731f7/ [Accessed: 14 June 2022].

Russian Federation (2015). 'National Security Strategy of the Russian Federation', Decree of the President of Russian Federation from 31.12.2015 N 683 [Указ Президента Российской Федерации от 31.12.2015 г. N 683]. [online] Available at: http://kremlin.ru/acts/bank/40391 [Accessed: 14 June 2022].

Russian Federation (2016a). 'Doctrine of Information Security of the Russian Federation', Decree of the President of Russian Federation from 05.12.2016 N646 [Указ Президента Российской Федерации от 05.12.2016 г. N 646]. [online] Available at: http://kremlin.ru/acts/bank/41460 [Accessed: 14 June 2022].

Russian Federation (2016b). Federal Law 'On Amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure public security' dated 06.07.2016 N 375-FZ [Федеральный закон 'О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности' от 06.07.2016 N 375-ФЗ] [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_201087/ [Accessed: 14 June 2022].

Russian Federation (2016c). Federal Law 'On Amendments to the Federal Law 'On Countering Terrorism' and Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Measures to Counter Terrorism and Ensuring Public Security' dated 06.07.2016 N 374-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'О противодействии терроризму' и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности' от 06.07.2016 N 374-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_201078/ [Accessed: 14 June 2022].

Russian Federation (2017d). Federal Law 'On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Code of Criminal Procedure of the Russian Federation in connection with the adoption of the Federal Law 'On the Security of the Critical Information Infrastructure of the Russian Federation' dated 26.07. 2017 N 194-FZ [Федеральный закон 'О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона 'О безопасности критической информационной инфраструктуры Российской Федерации' от 26.07.2017 N 194-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_220891/ [Accessed: 14 June 2022].

Russian Federation (2017e). Federal Law 'On the security of the critical information infrastructure of the Russian Federation' dated 26.07.2017 N 187-FZ [Федеральный закон 'О безопасности критической информационной инфраструктуры Российской Федерации' от 26.07.2017 N 187-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/ [Accessed: 14 June 2022].

Russian Federation (2019). Federal Law 'On Amending the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection' dated 01.05.2019 N 90-FZ [Федеральный закон 'О внесении изменений в Федеральный закон 'О связи' и Федеральный закон 'Об информации, информационных технологиях и о защите информации' от 01.05.2019 N 90-ФЗ]. [online] Available at: http://www.consultant.ru/document/cons_doc_LAW_323815/ [Accessed: 14 June 2022].

Russian Federation (2022). 'Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development'. [online] Available at: http://en.kremlin.ru/supplement/5770 [Accessed: 14 June 2022].

Shalal, A. (2017). 'Germany challenges Russia over alleged cyberattacks', Reuters. [online] Available at: www.reuters.com/article/us-germany-security-cyber-russia/germany-challenges-russia-over-alleged- cyberattacks-idUSKBN1801CA [Accessed: 14 June 2022].

Snidal, D. (1985). 'The game theory of international politics', World Politics, vol. 38 no. 1, pp. 25-37.

Soldatov, A., Borogan, I. (2018). 'Russia's approach to cyber: the best defence is a good offence', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 15–25. [online] Available at: www.iss.europa.eu/sites/default/files/EUISS Files/CP_148.pdf [Accessed: 14 June 2022].

State Duma of the Russian Federation (2022). Legislation initiative No. 113045-8 'On control over the activities of persons under foreign influence' [Законопроект № 113045-8 О контроле за деятельностью лиц, находящихся под иностранным влиянием]. [online] Available at: https://sozd.duma.gov.ru/bill/113045-8 [Accessed: 14 June 2022].

Stone, A. (2011). 'Cyberspace: The next battlefield', USA Today, June 19. [online] Available at: https://usatoday30.usatoday.com/tech/news/2001-06-19-cyberwar-full.htm [Accessed: 14 June 2022].

Tema, M. (2014). 'Basic assumptions in game theory and international relations', International Relations Quarterly, vol.5 no.1, pp. 1-5.

Tikk, E. and Kerttunen, M. (2020). 'Routledge Handbook of International Cybersecurity'. London: Routledge.

Trauner, F., Carrapico, H. (2012). 'The External Dimension of Justice and Home Affairs after the Lisbon Treaty: Analyzing the Dynamics of Expansion and Diversification', Foreign Affairs Review, no. 17, pp. 1–18.

Trejnis Z, Trejnis P. (2017). 'Polityka ochrony cyberprzestrzeni w państwie współczesnym', Studia Bobolanum, vol. 28 no. 3, p. 27.

UNGA (1999). 'Developments in the field of information and telecommunications in the context of international security'. UNGA A/RES/53/70. [online] Available at: https://undocs.org/A/RES/53/70 [Accessed: 14 June 2022].

UNGA (2013). 'Resolution A/68/98: report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security'. [online] Available at: www.un.org/ga/search/view_doc.asp?symbol=A/68/98 [Accessed: 14 June 2022].

UNGA (2015a). 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United

Nations addressed to the Secretary-General'. UNGA A/69/723. [online] Available at: https://undocs.org/A/69/723 [Accessed: 14 June 2022].

UNGA (2015b). 'Resolution A/70/174: report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security'. [online] Available at: www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [Accessed: 14 June 2022].

UNGA (2017). 'Letter dated 11 October 2017 from the permanent representative of the Russian Federation to the United Nations addressed to the Secretary-General'. UNGA A/C.3/72/12. [online] Available at: https://undocs.org/A/C.3/72/12 [Accessed: 14 June 2022].

UNGA (2018a). 'Resolution A/C.1/73/L.37: advancing responsible state behaviour in cyberspace in the context of international security'. [online] Available at: https://undocs.org/A/ C.1/73/L.37 [Accessed: 14 June 2022].

UNGA (2018b). 'Resolution A/RES/73/187: countering the use of information and communications technologies for criminal purposes'. [online] Available at: https://undocs.org/en/A/ RES/73/187 [Accessed: 14 June 2022].

UNGA (2018c). 'Resolution A/RES/73/27: developments in the field of information and telecommunications in the context of international security'. [online] Available at: https://undocs. org/A/RES/73/27 [Accessed: 14 June 2022].

UNGA (2019). 'Countering the use of information and communications technologies for criminal purposes: report of the secretary-general'. [online] Available at: https://undocs.org/en/A/74/130 [Accessed: 14 June 2022].

UNGA (2019). 'Resolution Countering the use of information and communications technologies for criminal purposes' UNGA 74/247. [online] Available at: https://undocs.org/A/Res/74/247 [Accessed: 14 June 2022].

UNGA (2021). 'Developments in the field of information and telecommunications in the context of international security', UNGA 76/135. [online] Available at: https://undocs.org/A/76/135 [Accessed: 14 June 2022].

Väljataga, A. (2017). 'Back to square one? The fifth UN GGE fails to submit a conclusive report at the UN general assembly', CCDCOE. [online] Available at: https://ccdcoe.org/back-square-one-fifth-un-gge-fails- submit-conclusive-report-un-general-assembly.html [Accessed: 14 June 2022].

Van Vooren, B. (2012). EU External Relations Law and the European Neighbourhood Policy. A Paradigm for Coherence. London: Routledge.

Vilmer, J.-B. (2018). 'Lessons from the Macron Leaks', in Popescu, N., Secrieru, S. (eds.) Hacks, leaks and disruptions Russian cyber strategies. Paris: Chaillot Paper, pp. 75–85. [online] Available at: www.iss.europa.eu/sites/default/files/EUISS Files/CP_148.pdf [Accessed: 14 June 2022].

Waltz, K. (1979). Theory of International Politics. Reading, Mass.: Addison-Wesley Pub. Co.