INTERNATIONAL COOPERATION IN ENSURING INTERNATIONAL INFORMATION SECURITY

By
Ian Kyslytsya

Submitted to
Central European University
Department of International Relations

In partial fulfilment of the requirements for the degree of
Master of Arts in International Relations

Supervisor: Professor Boldizsár Nagy

Vienna, Austria
2021

Abstract

Rapid progress in the field of information and communication technologies contributes not only to the economic, social and cultural development of states, but also leads to the emergence of new types of threats in the information space, the fight against which requires proper legal regulation. However, a global regime of information security ensured by international law has not emerged. This thesis is devoted to the legal analysis of existing international cooperation in the field of information security and based on a comparative analysis with the fields of nuclear arms control and remote sensing, demonstrates that the nature of international cooperation depends, first of all, not on the technological characteristics of the particular area in which cooperation is conducted, but on the nature of relations between key actors and the perception of their interests.

Table of Contents

Introduction

The omnipresent spread of information and communication technologies (ICT) in the economy, politics and social relations gives rise to information challenges and security threats. The problem of international information security (IIS) is acute; however, due to the transnational nature of the information sphere, it cannot be provided at the level of individual states and requires international answers. Thus, in recent years, the issue of international information security has attracted great attention at both the expert, academic and political levels.

International cooperation in the field of information security is reflected in the activities of such international organizations and forums as the United Nations, North Atlantic Treaty Organization, Shanghai Cooperation Organization and a number of others. Currently, the formation of a global information security regime is expected, similar to the regimes that have developed in other high-tech areas of world politics, that should take into account the development and regulation of the global information space.

In this regard, many scholars consider the applicability of certain legal instruments of international cooperation to the information sphere. The problems of developing a regulatory framework for ensuring information security in the international arena are covered by such authors as Martha Finnemore and Henry Farrell.[1] The study of the applicability of confidence-building measures to cybersecurity is discussed by James Lewis and Jason Healey.[2] Additionally, Joseph Nye engages in the analysis of international cooperation in this area from the standpoint of the theory of international regimes.[3]

---

[1] Martha Finnemore, "Cultivating International Cyber Norms." *America's Cyber Future: Security and prosperity in the Information Age* 2 (2011): 89-100. Henry Farrell. *Promoting Norms for Cyberspace*. Council on Foreign Relations, 2015.

[2] James Lewis, "Confidence-building and international agreement in cybersecurity." *Disarmament Forum* 4 (2011): 51-59. Jason Healey, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd, "Confidence-building Measures in Cyberspace." *Atlantic Council, Brent Scowcroft Center on International Security* (2014).

[3] Joseph Nye, "The Regime Complex for Managing Global Cyber Activities", Vol. 1. *Belfer Center for Science and International Affairs*, (John F. Kennedy School of Government, Harvard University, 2014).

There is also a strong trend in the international relations scholarly work associated with techno-optimism,[4] arguing that global politics in the context of the information revolution and, in particular, international political relations regarding the regulation of ICTs should qualitatively and for the better differ from the previous stages of the development of world politics. This is part of a more general structuralist argument, according to which the features of the structure of social interaction determine its patterns. However, based on this assertion, the existing structure of the infosphere should favor information security cooperation as much as possible, yet a global regime of international information security has not emerged.

An analysis of scholarly sources and official documents on the problems of ensuring international information security shows that the issues of finding the optimal conceptual design and identifying promising areas of cooperation in theoretical terms are not comprehensively covered in the academic literature. This thesis intends to fill this gap.

This thesis will argue that the negotiation process will continue until an acute international crisis establishes a balance of terror between the parties and only then international cooperation will enter the implementation phase, which, given the importance of this issue, promises to be effective. Escalating interstate conflicts and the arms race in the infosphere will create conditions for the transition from the negotiation phase to the implementation of agreements.

The methodological approach of this thesis will be based on the so-called Social Theory of International Politics,[5] in particular, the theory of social constructivism.[6] Such an approach presupposes tracing backward and forward linkages between objective and subjective dimensions

---

[4] Alvin Toffler, *Powershift : Knowledge, Wealth, and Violence in the 21st Century* (New York: Bantam Books, 1990), 640. Manuel Castells, "Communication, Power and Counter-power in the Network Society," *International Journal of Communication* 1, no. 1 (2007): 238-266.

[5] Alexander Wendt, *Social Theory of International Politics* (Cambridge, UK : Cambridge University Press, 1999).

[6] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International organization* 52, no. 4 (1998): 887–917. Friedrich V. Kratochwil, R*ules, Norms, and Decisions : on the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs* (Cambridge University Press, 1991).

(identity, perceptions, discourses) of the international political reality. This approach is especially well suited for studying information security issues due to the fact that the global information space is an area of global politics, constructed as a result of human activity.

This thesis will rely on Oran R. Young's approach of institutional bargaining in regime theory, which identifies three stages that each regime goes through in its formation: setting the agenda, negotiation and agreement implementation.[7] To analyze the negotiation process, the theory of international cooperation will be used within the framework of the "bargaining" model, developed by such authors as James Fearon,[8] Diana Panke[9] and Sebastian Rosato.[10] According to this approach, cooperation in all areas has the same sequence, consisting of two phases: bargaining and implementation. At the same time, the negotiation phase of cooperation within the framework of this approach is described by the "attrition warfare"[11] model. If the subject of cooperation for the actors is of significant interest, then the attrition warfare will last for a rather long time and the actors may not get to the implementation phase. However, in conditions where the negotiators feel mutual vulnerability, the likelihood of reaching effective agreements increases significantly. This theory refutes the widespread belief in the academic literature that international cooperation in each individual area (trade, nonproliferation, ecology, etc.) is determined by the characteristics of the strategic structure of this area.[12] In other words, the longer the "shadow of the future"[13] from the subject of negotiations (that is, the more

[7] Oran R. Young, *International Cooperation : Building Regimes for Natural Resources and the Environment* (Ithaca: Cornell University Press, 1989).

[8] James D. Fearon, "Bargaining, Enforcement, and International Cooperation." *International Organization* 52, no. 2 (1998): 269–305.

[9] Diana Panke, "Lock-in Strategies in International Negotiations: The Deconstruction of Bargaining Power." *Millennium* 43, no. 2 (2015): 375–391.

[10] Sebastian Rosato, "The Inscrutable Intentions of Great Powers." *International Security* 39, no. 3 (2015): 48–88.

[11] *The International Encyclopedia of the First World War* defines attrition warfare as "the sustained process of wearing down an opponent so as to force their physical collapse through continuous losses in personnel, equipment and supplies."

[12] Helen Milner, "International Theories of Cooperation among Nations: Strengths and Weaknesses." *World Politics* 44, no. 3 (1992): 466-496.

[13] The shadow of the future is a basic game theory concept which expresses the idea that we behave differently when we expect to interact with someone repeatedly over time.

significant the issue is under discussion for the actors), the less likely there will be a conclusion of a working agreement. However, if such an agreement is nevertheless reached, then, given the high interest of the actors, there should be no problems in its implementation.

The institutional bargaining approach of Young's theory of regimes and Fearon's concept in a similar way understand the logic of international cooperation. Their joint use allows, on the one hand, to analyze in detail international cooperation in ensuring information security in different regions, as well as to analyze international cooperation in other high-tech areas of world politics, and on the other, make predictions based on the analysis of the strategic structure of relations between the most influential actors in the framework of the international information security regime.

The traditional security paradigm, according to the neorealist approach,[14] will be used to analyze the formation of the existing contradictions in international cooperation in ensuring information security. This concept of securitization makes it possible to analyze the process of forming the agenda, current foreign policy and the research discourse in the field of IIS.

This thesis will also apply the "case-study" approach.[15] From the standpoint of this theory, international cooperation in the field of information security is a deviating case, since infosphere experts consider cooperation in this area as fundamentally different from other areas of international politics.[16]

The first chapter of the thesis will analyze the concept of international information security, highlight the main stages of the formation and development of IIS in international law and assess their impact on the evolution of international cooperation. The second chapter will review existing multilateral and bilateral levels of cooperation in ensuring IIS. And the third chapter, using a comparative analysis of international cooperation in the field of information

[14] John Mearsheimer, *The Tragedy of Great Power Politics*. (WW Norton & Company, 2001).

[15] John Gerring, *Case Study Research : Principles and Practices* (New York: Cambridge University Press, 2007).

[16] Andrew Chadwick and Philip N. Howard. *Routledge Handbook of Internet Politics* (London: Routledge, 2009). Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, Mass: MIT Press, 2012).

security, nuclear arms control, as well as remote sensing of the Earth from Outer Space, will identify the promising trends in the formation of a global international regime for ensuring information security.

CHAPTER 1: THE CONCEPT AND DEVELOPMENT OF INTERNATIONAL INFORMATION SECURITY

In the digital age, the essence of security has not changed. Arnold Wolfers' definition of national security as the absence of threats to the core values of society remains valid.[17] However, the nature of challenges and threats have changed as well as the conditions and means of ensuring security. The composition and nature of the relationship between security actors is also undergoing transformation. In these conditions, the perception by states of the priority of threats to international and national security is changing, which in turn affects the nature of international cooperation. An integral part of modern "information warfare"[18] are "information weapons",[19] which also act as elements of interstate competition during peacetime. As a result, an information and cyber arms race has emerged.[20]

There are several key features of the information sphere that affect the perception of threats to IIS by states:

- the problem of unambiguously identifying the source of an attack (the problem of attribution) in the information space;[21]

- the transboundary nature of the information space and the interdependence of states in this area increases the vulnerability of state and non-state actors;

[17] Arnold Wolfers, ""National security" as an Ambiguous Symbol." *Political Science Quarterly* 67, no. 4 (1952): 482.

[18] At present, there is no generally accepted definition of information warfare and information weapons. For the purpose of this thesis, information warfare assumes a confrontation between two or more states in the information space with the aim of damaging information systems, processes and resources, critical infrastructure, undermining political, economic and social systems, psychologically manipulating masses of the population to destabilize society and the state.

[19] Information or cyber weapons are ICTs used for the purpose of information warfare.

[20] Axel Wirth, ""The Cyber Arms Race Is On': Lessons from the U.S. Presidential Election." *Biomedical Instrumentation & Technology* 50, no. 6 (2016): 463–465.

[21] Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyber Space: The Evolving International Law of Attribution," *Fletcher Security Review* 55-73 (2014): 19.

- the "security dilemma" in the information sphere is acute, due to the asymmetry of the defensive and offensive potential of cyber and information weapons;[22]

- protected and unprotected objects of critical infrastructure in the information space are closely intertwined; in information warfare, it is difficult to distinguish between civilian and military objectives, which complicates regulation of this area and leads to the fact that information attacks can be carried out in peacetime, as part of interstate competition.

The above-mentioned features complicate international cooperation in ensuring information security, since they create difficulties in monitoring the agreements reached and assessing the intentions of the participants.[23] However, as James Fearon convincingly argues,[24] despite the significance of the specificity of the object of regulation, the perception of the significance of the problem by the subjects of interaction has the greatest influence on the nature and prospects of international cooperation.

Today, there are three main groups of threats to international information and cyber security, determined by the nature of the goal setting of their subjects - information crime, information terrorism and information warfare.[25] At the same time, most researchers agree that, despite the importance of the first two, it is the military-political dimension of information security that poses the greatest threat to international peace and stability.[26]

The securitization of the global information space is becoming a response to the cross-border nature of information challenges and threats. However, securitization practices proceed from different identities and, as a consequence, interpretations of the national interests of states that act as securitizing actors. The ultimate goal is similar for all states - it is the restoration of

[22] Martin C. Libicki, "Is There a Cybersecurity Dilemma?" *The Cyber Defense Review* 1, no. 1 (2016): 129-140.

[23] Joseph M Grieco, "Anarchy and the Limits of Cooperation: a Realist Critique of the Newest Liberal Institutionalism." *International Organization* 42, no. 3 (1988): 485-507.

[24] Fearon, "Bargaining, Enforcement, and International Cooperation.", 270-276.

[25] General Assembly resolution 54/49, *Developments in the field of information and telecommunications in the context of international security*, A/RES/54/49 (23 December 1999).

[26] Görz Neuneck, "Civilian and military cyberthreats: shifting identities an attribution." *The Cyber Index. International Security Trends and Realities. UNIDIR* (2013): 115.

state sovereignty in the information space, the use of force, as well as strengthening the borders of regions and the formation of communities of states within the region adhering to similar interpretations of threats to IIS and pursuing a similar policy in this area.[27]

1.1 Cybersecurity vs Information Security

There are two competing securitizing discourses in the field of information security, which determine in different ways the nature of threats to national and international security. These two discourses are associated with divergences in states' approaches to defining ICT threats to be resolved at the international level, and they are also widely represented in the academic literature.

The mainstream approach in the so-called Western world is to define the scope of such security problems and threats through the discourse of "cybersecurity".[28] The US National Institute of Standards and Technology glossary of key information security terms defines cybersecurity as "the ability to protect or defend the use of cyberspace from cyber attacks".[29] European scholars in the vast majority of cases when using the term "cybersecurity", refer to "the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace".[30] In this regard, the European Union's cybersecurity strategy defines it as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its

[27] Andrew Liaropoulos, "Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?" *Journal of Information Warfare* 12, no. 2 (2013): 21-23.

[28] Johan Eriksson and Giampiero Giacomello, eds. *International Relations and Security in the Digital Age*. Vol. 52. (Routledge, 2007): 12.

[29] Celia Paulsen and Robert Byers. *Glossary of key information security terms*. NIST Internal or Interagency Report (NISTIR) 7298 Rev. 3. National Institute of Standards and Technology, 2019.

[30] Rossouw Von Solms and Johan Van Niekerk, "From information security to cyber security." *Computers & Security* 38 (2013): 101.

interdependent networks and information infrastructure".[31] Evidently, the cybersecurity discourse is primarily focused on ensuring information and technical security, which includes protection, control and compliance law in the infosphere, although the openness of information flows on a global scale is also considered as a referent object of security.

The discourse of "information security", is the approach of China and Russia,[32] a number of Arab and Latin American countries.[33] Such a discourse encompasses not only information and technical, but also psychological security, which implies the protection of both the society and the state from negative information influences and the protection of "digital sovereignty".[34]

Within the framework of the United Nations, the development of a common terminology and definitions in the field of IIS was first analyzed by the UN Group of Governmental Experts (GGE). The search by GGE members for mutually acceptable definitions in order to find a compromise led to the fact that the texts of UN resolutions do not use the term "information security" or "cybersecurity", instead relying on the term "information and communication technologies in the context of international security".[35]

As shown, scholars and experts of international organizations conceptualize this field differently. Often, they use different terms to define the same concept. For the purpose of this thesis, "international information security" is defined as a state of affairs provided by obligations

---

[31] *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 of the European Commission and Higher Representative for foreign affairs and security policy. Brussels* (2013).

[32] International Strategy of Cooperation on Cyberspace. Ministry of Foreign Affairs of the People's Republic of China. Beijing, 2017. David Gorr and Wolf J Schünemann, "Creating a Secure Cyberspace – Securitization in Internet Governance Discourses and Dispositives in Germany and Russia". *The International Review of Information Ethics* 20 (Edmonton, Canada 2013): 37-51.

[33] Fathiya Al Izki and George Weir, "Information security and digital divide in the Arab world." In Cyberforensics 2014-International Conference on Cybercrime, *Security & Digital Forensics* (2014): 15-24. Radomir Bolgov, "The UN and Cybersecurity Policy of Latin American Countries." *In 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG*) (2020): 259-263.

[34] Julia Pohle and Thorsten Thiel. "Digital Sovereignty". *Internet Policy Review* 9, no. 4 (2020).

[35] United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*: *note by the Secretary-General*, A/70/174 (22 July 2015).

created by international law, which prevents violation of international peace and ensures security of both individual states and the world community as a whole in the field of ICTs.

1.2 Formation and Development of Information Security in International Law

The set of threats that arose with the beginning of a large-scale introduction of ICTs gave impetus to the process of the formation and development of IIS in the framework of international law. However, international agreements on IIS differ in status, range of participants, substantive scope, perfection of wording and terminology. All this creates significant difficulties in the perception and application of these international agreements.

An important event in the history of IIS was the 1990 8th United Nations Congress on Crime Prevention and Criminal Justice, the largest intergovernmental forum influencing both national policies and the development of recommendations for international cooperation. For the first time among other topics in the fight against transnational crime, it had addressed the issue of computer-related crime.[36] The 8th UN Congress recognized the need to reach an international consensus on the types of computer crimes that must be recognized as criminal offenses in all member states in order to punish the perpetrators.[37] Evidently, in the early 1990s, the state was not mentioned as a subject of computer crimes.

From the early 2000s to 2010, foundations of IIS were formed within international organizations. As it was during this period that the global information society was formed, as evidenced by the adoption of such important documents as the Okinawa Charter and the Millennium Declaration,[38] the 10th UN Congress on the Prevention of Crime and the Treatment of Offenders and the two stages of the World Summit on the information society in Geneva and

[36] General Assembly resolution 45/109, *Computerization of criminal justice*, A/RES/45/109 (14 December 1990).

[37] General Assembly resolution 45/121, *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, A/RES/45/121 (14 December 1990).

[38] *The Okinawa Charter on the Global Information Society*, Kyushu-Okinawa Summit 2000, 23 July 2000. *Millennium Declaration,* Millennium Summit of the United Nations New York, 6-8 September 2000.

Tunisia.[39] In this period, the issues of cooperation between states in the field of IIS come to the fore. The 10th UN Congress showed that there has been a significant evolution of information crimes, both in terms of quantity and complexity. All these factors contributed to the drafting of the first relevant international legal documents within regional organizations, namely: the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information,[40] The Council of Europe Convention on Cybercrime,[41] and the Agreement between the Governments of the Shanghai Cooperation Organization Member States on Cooperation in the Field of International Information Security.[42] In them, states were finally recognized as full subjects of illegal actions in the information space.

Although the process of further development of relevant international law at the regional level continues to this day, as evidenced by the international legal instruments adopted within regional organizations, such as the 2010 Convention on Combating Information Technology Offences of the Arab League,[43] 2014 African Union Convention on Cyber Security and Personal Data Protection,[44] and the EU Directive on Security of Network and Information Systems (NIS Directive).[45] Over the past decade, concrete proposals for a universal international agreement in the field of IIS under the auspices of the UN emerged, such as the 2011 draft Convention on International Information Security[46] and the draft Global Agreement on Cybersecurity and

[39] United Nations, *Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,* A/CONF.187/15 (10-17 April 2000). General Assembly resolution 56/183, *World Summit on the Information Society,* A/RES/56/183 (31 January 2002).

[40] Commonwealth of Independent States*, Agreement on Cooperation in Combating Offences related to Computer Information*, June 1 2001.

[41] Council of Europe, *Convention on Cybercrime*, 23 November 2001.

[42] Shanghai Cooperation Organisation, *Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security*, Yekaterinburg, 16 June 2009.

[43] League of Arab States, *Arab Convention on Combating Information Technology Offences*, 21 December 2010.

[44] African Union, *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014.

[45] European Union, *Directive on Security of Network and Information Systems (NIS Directive)*, 6 July 2016.

[46] The Ministry of Foreign Affairs of the Russian Federation, *CONVENTION ON INTERNATIONAL INFORMATION SECURITY (Concept)*, 22 September 2011.

Cybercrime.[47] The form, substantive scope and terminology are still the subject of dispute between the participants in the international arena, but the need for such a document is recognized by all countries. In addition, there are suggestions for the establishment of an independent international organization on cybersecurity, as well as an international criminal tribunal for cyberspace.[48] At present, these are only academic proposals, but modern realities and the development by states of not only defensive but also offensive information strategies in recent years dictate the urgent need to solve the problem of providing IIS at the universal level.[49]

[47] Stein Schjolberg and Solange Ghernaouti-Helie, "A Global Treaty on Cybersecurity and Cybercrime." *Cybercrime Law* 97 (2011): 9-14, https://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf

[48] Nazli Choucri, Stuart Madnick and Jeremy Ferwerda, "Institutions for cyber security: International responses and global imperatives." *Information Technology for Development* 20, no. 2 (2014): 96-121.

[49] Max Smeets, "Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment." *Defence Studies* 18, no. 4 (2018): 395-410.

CHAPTER 2: EXISTING COOPERATION IN ENSURING INTERNATIONAL INFORMATION SECURITY

2.1 Universal Level of Cooperation

Within the framework of the United Nations, the issue of ensuring IIS was first considered in 1999 during the 53rd session of the UN General Assembly. The dual nature of the achievements of science and technology in the civilian and military spheres was recognized by Resolution 53/73.[50] It was supported by 77 states, mostly from South America, Africa, the Pacific and the Middle East. 43 stated voted against, predominantly from North America, Europe, Australia and New Zealand. 16 states abstained. Nevertheless, this showed the readiness of the vast majority of states to intensify joint efforts in order to counter transnational threats from the use of ICT in order to solve the problem of IIS with the maximum consideration of all stakeholders.

In 2003, the 58th session of the UN General Assembly adopted Resolution 58/32,[51] which facilitated the transition of IIS issues from general political discussion to practical solutions and launched a mechanism for forming the GGE. The UN GGE clearly established that international law, namely the UN Charter and the basic principles of international law, also applies to the information space. The group also recognized that the subjects of threats in the information space can be both state and non-state actors and that ICTs can be used as a tool of warfare.[52] However, it is on this platform, where the two competing discourses discussed in Chapter 1 based on different interpretations of referent security objects actively collide. During the discussions on the mandate of the GGE in 2017 the debate about whether the group should

[50] General Assembly resolution 53/73, *Role of science and technology in the context of international security and disarmament*, A/RES/53/73 (4 January 1999).

[51] General Assembly resolution 58/32, *Developments in the field of information and telecommunications in the context of international security*, A/RES/58/32 (8 December 2003).

[52] General Assembly resolution 69/28, *Developments in the field of information and telecommunications in the context of international security*, A/RES/69/28 (2 December 2014).

discuss only issues of ensuring the security of critical infrastructures (information technology component of security) or content issues (socio-humanitarian component) effectively paralyzed its work.[53]

In December 2018, the UN General Assembly established the Open-Ended Working Group (OEWG) tasked to continue to develop the rules, norms, and principles of responsible behavior of states, discuss ways for their implementation, and to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the UN.[54] Thus, two UN platforms for international cooperation on the same issue are being formed, which indicates that the global dialogue in this area is disintegrating.

In order to overcome the differences, it may be possible to harmonize the work of the OEWG and the GGE. The OEWG could focus on major political topics that concern most members of the international community - the framework on responsible state behavior in the information space, confidence-building measures in this area, as well as on proposals for the negotiation format itself (a permanent committee of the General Assembly or the UN Security Council). The GGE, in turn, could, as a priority, tackle an equally important but more narrowly specialized topic - the applicability of existing international law to the information space. Thus, opportunities for dialogue and harmonization of approaches remain.

As the only organization with universal membership and indisputable legitimacy, the UN is the central negotiating platform where the problems of ensuring IIS are discussed. However, at the universal level there is still no conventional mechanism for its ensurance. Differences in the positions of states lead to the fact that most of the documents adopted within the framework of the UN are of a recommendatory nature. These documents are acts of "soft law", which

[53] Stefan Soesanto and Fosca D'Incau, "The UN GGE Is Dead: Time to Fall Forward," *European Council on Foreign Relations*, August 15, 2017, https://ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance/

[54] General Assembly resolution 73/27, *Developments in the field of information and telecommunications in the context of international security*, A/RES/73/27 (5 December 2018). In December 2020, the OEWG was renewed for 2021-2025. General Assembly resolution 75/240, *Developments in the field of information and telecommunications in the context of international security*, A/RES/75/240 (31 December 2020).

reflect only the promising areas of development of legal regulation of the problem of providing IIS at the universal level.[55] However, in the future they can serve as a legal basis for concluding a single agreement on IIS.

2.2 Multilateral and Bilateral Levels of Cooperation

The absence of an institutionally or formally fixed regime often reflects the interests of individual states seeking to retain leadership in the relevant area.[56] States support the formation of a multitude of disparate organizations and institutions that regulate interaction in the same area of international relations since this allows one to choose different norms and rules of interaction enshrined in these agreements, depending on situational interests.

Analysis of the main normative documents and activities of regional organizations in the field of IIS shows that among the large number of international organizations, only five have adopted international conventions on information security.[57] These documents differ significantly in the subject of their regulation, reflect regional approaches to understanding IIS, and provide for different forms of cooperation. At the same time, experts name the United States, China, Russia and the EU+UK, as the most active participants in the IIS negotiation process.[58] Among them, major contradictions exist, which are viewed as a key obstacle to productive international cooperation.[59] The reasons for the contradictions are, on the one hand, interstate competition and the struggle for influence in the international arena, and on the other, the difference in potentials and, as a consequence, interests in the information sphere.

[55] Kubo Mačák, "From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers." *Leiden journal of international law* 30, no. 4 (2017): 877–899.

[56] Marc L. Busch, "Overlapping institutions, forum shopping, and dispute settlement in international trade." *International Organization* (2007): 735-761.

[57] See Chapter 1.2.

[58] Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." *In 2013 5th International Conference on Cyber Conflict* (CYCON 2013): 1-17.

[59] Ronald Deibert, "Trajectories for Future Cybersecurity Research." *In The Oxford Handbook of International Security*. (2018): 531-556.

Russia aims to limit possible national security risks associated with the information space by consolidating the principle of non-interference in the information space - in accordance with the draft Convention on international information security submitted to the UN by Russia "each State has the right to make sovereign norms and govern its information space according to its national laws".[60] China, like Russia, advocates state regulation of the information sphere and ensuring information security on the basis of international treaties. In 2015, Russia and China signed an agreement on cooperation in the field of international information security containing common definitions of threats to information security.[61] This agreement can be interpreted as the desire of these states to undermine the leading positions of the United States in the field of Internet governance and IIS.[62] It should be noted that Russia and China are putting forward similar initiatives on information security at BRICS and SCO.[63] However, the position of China in comparison with the Russian one is distinguished by greater expectancy,[64] despite the fact that the contradictions are not only political, but also economic in nature.[65]

The theoretical foundations of US IIS foreign policy strategy were formulated by Joseph Nye, who points to the possibility of applying the current nuclear deterrence strategy to cyberspace. As Nye notes,[66] cyber deterrence includes retaliation (including the need to publicly voice the threat of imminent retaliation in response to a successful cyberattack), cyber defense

---

[60] The Ministry of Foreign Affairs of the Russian Federation, CONVENTION ON INTERNATIONAL INFORMATION SECURITY (Concept), 22 September 2011.

[61] Government of the Russian Federation, *On the signing of an Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security*, Moscow, 30 April 2015, https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf.

[62] Tom Risen, "China, Russia Seek New Internet World Order." *US News and World Report* 14 (2015).

[63] Luca Belli, *CyberBRICS : Cybersecurity Regulations in the BRICS Countries* (Cham, Switzerland: Springer, 2021). United Nations, General Assembly, *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*, A/69/723 (13 January 2015).

[64] Stanislav Budnitsky and Jia Lianrui, "Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance." *European Journal of Cultural Studies* 21, no. 5 (2018): 594-613.

[65] Kadri Kaska, Henrik Beckvard and Tomas Minarik, "Huawei, 5G and China as a security threat." *NATO Cooperative Cyber Defense Center for Excellence* (CCDCOE, 2019).

[66] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (2016): 44-71.

(increasing the resilience and security of information networks in order to minimize the benefits of an offensive cyber weapon can receive), interdependence between allies and potential enemies in order to increase the costs of information warfare, support and development of international rule-making (the development of international cooperation in the field of applicability of humanitarian law to the information sphere). The United States proceeds from the fact that in cyberspace, given the difficulty of verifying the source of an attack and inspections, it is impossible to limit weapons. However, it is feasible to limit the probable targets of cyberattacks enshrined in norms of international law. Under these conditions, it is possible to establish a normative taboo on cyberattacks against civilian infrastructure and civilians. This prohibition could be strengthened by the development of confidence-building measures in cyberspace, such as international assistance in collecting the evidence needed to attribute a cyberattack. Thus, in this way norms of international humanitarian law are extended to the cyberspace without adapting them to the specifics of this area. However, for many years a private sector based model of regulation was suggested and the military-political component of information security was avoided.[67] The official position on this issue changed during the Obama administration. It is indicative that in 2015 the Cyber Strategy of the US Department of Defense for the first time mentioned the aggressive actions of Russia and China in the cyberspace as well as threats emanating from Iran and the DPRK as the main threats to US national security.[68] In addition, a threshold was set for cyberattacks in response to which retaliatory measures will be taken, including the use of conventional weapons. The change in the position of the United States on the issue of ensuring information security was the result of a change in the balance of power due to the rapid development of China's cyber potential. In the US research community discussions

[67] Kenneth Lieberthal and Peter Warren Singer, *Cybersecurity and US-China relations*, (Brookings, 2012).

[68] The Department of Defense Cyber Strategy, Washington, April 2015.

are underway about the forms of possible cyber clashes with China,[69] and analytical reports indicate a significant number of cyber attacks by Chinese hackers on critical US infrastructure.[70]

As a rule, the approach of EU member states, which also act as influential players in the global information space, can be interpreted as similar to the approach of the United States. Mainly because of the allied commitments to NATO as well as due to significant interdependence in the economic aspects of the development of the ICTs. As evidenced by the EU cyberstrategy,[71] member states show concern, first of all, towards protecting the economy from information threats. At the same time, international negotiations during the NETmundial Initiative[72] have shown that European countries, primarily Germany and France, are gravitating towards more independent information security policies. Experts associate such a change in positions with the revelations of Edward Snowden,[73] who pointed to the fact that the United States was using its advantages in the information sphere in order to obtain political, economic and political goals to the detriment of the interests of the EU countries. In this regard, the initiative of France voiced during the Forum on Internet Governance in Paris in 2018 should be noted. According to the "Paris Call for Trust and Security in Cyberspace",[74] while the importance of international cooperation at the UN is recognized, such interaction must be carried out in a multi-level format, with the participation of all states, business and civil society.

[69] Yavuz Akdag, "The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective." *Journal of Chinese Political Science* 24, no. 2 (2019): 225-247.

[70] "Significant Cyber Incidents," *Center for Strategic and International Studies*, May 24 2021.

[71] European Commission, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade*, Brussels, 16 December 2020.

[72] An internet governance conference held by the Brazilian government and DNS overseer ICANN in May 2014.

[73] Derrick L. Cogburn, "Relinquishing the Root: Snowden, NETmundial, and the IANA Transition." *In Transnational Advocacy Networks in the Information Society*, (Palgrave Macmillan, New York, 2017): 248.

[74] France Diplomatie. *Paris Call for Trust and Security in Cyberspace*, 12 November 2018.

For developing countries in the course of international negotiations, priority is given to the issues of information development and the reduction of the "digital divide", including assistance in creating "digital potentials".[75]

Currently, new opportunities are opening up for the formation of a global regime of international information security. The change in the nature of threats to information security has led to the fact that the most developed states in terms of information are extremely vulnerable.[76] Thus, many key contradictions are currently fading into the background. However, new disagreements have also emerged due to the position of NATO countries on the international legal regulation of the military-political aspect of information security, reflected in the Tallinn Manual originally published in 2013 and later revised in 2017.[77] This document, prepared by a group of experts from the NATO Cooperative Cyber Defense Center in Tallinn, is devoted to the application of existing international law to information warfare, primarily in its technological dimension. According to the official position of Russia,[78] this Manual allows for the possibility of militarizing the information space, while Russia emphasizes the need for a complete ban on such activities.

Western and Russian/Chinese approaches do not necessarily contradict each other. It is indicative that both groups of states advocate the adoption of norms and rules of behavior of states in the information space, however, their approaches to the content of such norms differ significantly. Russia advocates the development of framework rules of conduct that would cover all aspects of IIS (protection of critical infrastructures, international Internet governance, issues of applicability of international law in the information sphere) and would harmonize the

[75] Ellada Gamreklidze, "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia." *Journal of International Communication* 20, no. 2 (2014): 200–217.

[76] Julia E. Sullivan and Dmitriy Kamensky, "How Cyber-attacks in Ukraine show the Vulnerability of the US power grid." *The Electricity Journal* 30, no. 3 (2017): 30-35.

[77] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (New York: Cambridge University Press, 2013). Michael N. Schmitt, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. (Cambridge University Press, 2017).

[78] Katarzyna Kubiak, "Towards a More Stable NATO-Russia Relationship." *European Leadership Network* (2019).

provisions of all existing regional regimes. At the same time, Russia proceeds from the premise that the rules should be of a peacekeeping nature, that is, they should be aimed at preventing conflicts in the information sphere. Thus, Russia proposes to form a comprehensive system of IIS and, for this purpose, to adapt existing international law to conflicts in the information sphere. China is in solidarity with the position of Russia. The United States and NATO, on the contrary, proceed from the fact that it is necessary to develop functional cooperation (create independent regimes aimed at ensuring the security of critical information infrastructures) and, at the same time, accept the possibility of applying norms and principles of existing international humanitarian law to regulate the military use of ICTs without adapting them. [79]

Rapprochement and harmonization of the two approaches is a long-term task, caused by the lack of trust between the key negotiators. The conclusion of bilateral agreements on information security can create the atmosphere of confidence necessary for the continuation of negotiations.[80] Within the framework of the emerging regime of ensuring international information security, the common interest of states should be the establishment of a robust atmosphere of trust and strengthening of online relations. This is achieved by using principles, norms, rules and decision-making procedures to protect confidentiality, integrity and privacy of information.[81] And the adoption of rules of conduct for states in this area can be an important step towards the development of international cooperation.

The convergence of the securitizing discourses of the United States, on the one hand, and Russia and China, on the other, would form the political basis of an international regime at the universal level. The first steps in this direction were already taken in 2018, when the UN

[79] Paul J. MacKenzie, "NATO's Vision and Strategy on the Cyberspace Domain", *Journal of the Japcc,* no 28 (2019): 16-22. Steven Hill, "NATO and the International Law of Cyber Defence." *Research Handbook on International Law and Cyberspace (2nd edition)*(2020 Forthcoming) (2020): 10-13.

[80] James Lewis, "Confidence-building and International Agreement in Cybersecurity." *Disarmament Forum* 4 (2011): 51-59. Jason Healey, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd, "Confidence-building measures in Cyberspace." *Atlantic Council, Brent Scowcroft Center on International Security* (2014).

[81] Friedrich V. Kratochwil, Rules, *Norms, and Decisions : on the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs* (Cambridge University Press, 1991).

General Assembly adopted a resolution containing the initial set of rules of conduct for states in the field of ICTs in the context of IIS.[82]

[82] General Assembly resolution 73/27, *Developments in the field of information and telecommunications in the context of international security*, A/RES/73/27 (5 December 2018).

CHAPTER 3: PROSPECTS FOR THE DEVELOPMENT OF A GLOBAL INFORMATION SECURITY REGIME

To identify the prospects for the development of a global information security regime, it is advisable to refer to the precedents of international cooperation in other high-tech areas: the field of nuclear arms control and remote sensing of the Earth from Outer Space.

3.1 Foundations of the Nuclear Arms Control Regime

The nuclear revolution that took place seven decades ago makes it possible to formulate some conclusions regarding the prospects for the development of a global IIS regime. In this regard, Joseph Nye compares the evolution of international cooperation in the field of nuclear arms control and cybersecurity.[83] Nye points out that strategic cybersecurity research in the early 2010s is in many ways similar to nuclear research in the 1950s and 60s, when experts could not draw unambiguous conclusions about the offensive and defensive capabilities of new weapons, the nature of deterrence in the international arena, the likelihood of escalation of conflicts, norms of behavior as well as the possibility of control over a new type of weapons.

At the agenda-setting stage of the formation of the nuclear arms control regime in the absence of a balance of power, the United States was interested in consolidating its own leadership in the new area. The goal of American initiatives was to place nuclear energy under international control in accordance with the Baruch Plan.[84] Proposed by the United States at the UN Commission on Atomic Energy in 1946, the Plan envisaged the introduction of a mechanism to control the nuclear programs of those who joined it and international inspections. It provided for the creation of an International Atomic Agency with broad rights and a high degree of autonomy (decisions in the agency had to be made by a simple majority of votes); the

[83] Joseph Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (2011): 18-38.

[84] David W Kearn Jr, "The Baruch Plan and the Quest for Atomic Disarmament." *Diplomacy & Statecraft 21*, no. 1 (2010): 41-67.

transfer of control to this agency over the production of fissile materials and their movement from one country to another; the transfer of research and development in the nuclear field under the agency's control; the provision by the United States to the disposal of the agency technological information on atomic energy for its joint use by participating countries. However, this proposal was perceived by the USSR as an attempt to limit the development of Soviet nuclear potential and a solidification of the US monopoly in the nuclear field. As a result, it was never implemented.

As the international regime develops, inevitably technology diffuses, which in turn contributes to the development of the international regime. After the nuclear revolution and the development of nuclear weapons delivery systems in the 1960s, a stalemate of mutual assured destruction occurred. An important factor that contributed to the formation of an international nuclear arms control regime was the recognition of mutual vulnerability on the part of the USSR and the United States.

The invention of the hydrogen bomb and its delivery vehicles in the USSR in 1955 changed not only the balance of power, but also the idea of the possibility of victory in a potential war. After the Cuban Missile Crisis in 1962, in the context of understanding the dangers of an escalation of a conflict between the nuclear superpowers, the perceptions and expectations of states began to converge, which became the basis for the formation of an international regime in this area. An important result was the creation of confidence-building measures, namely, a "hot line" between Moscow and Washington. Moreover, during this period foundations were laid for a non-proliferation regime. The understanding has come that the proliferation of nuclear technologies cannot remain peaceful and runs counter to the goals of maintaining international security.

A similar situation is emerging in the information sphere today. As discussed in Chapter 2 of this thesis, it is the awareness of vulnerability that pushes the United States to recognize the

military-political component of IIS threats, as well as to more international cooperation. The similarity of international cooperation in the field of nuclear arms control and information security lies in the fact that in both areas there is an asymmetry between the offensive and defensive capabilities of states - offense can be much more effective than defense.[85] The sabotage of nuclear power plants in Iran suggests possible directions of cyber conflicts directed against critical information infrastructures, but, according to experts,[86] do not reflect the full range of their capabilities. Despite the fact that some experts argue that changing the technical parameters of the Internet (protocols) will make it possible to identify the sources of the attack,[87] thus reducing the vulnerability of the most developed countries, today the trends in the development of the internet indicate that vulnerabilities in the infosphere will only increase.[88]

As with nuclear arms control, in the infosphere, international cooperation will rely more on the expectation and perception of threats than on experience. Nuclear weapons were used only against the Japanese cities of Hiroshima and Nagasaki in 1945; all subsequent containment strategy and instruments of international cooperation were built on the basis of ideas about the possible features of a nuclear war. This is the reason why it is especially important to study the perception of threats and the rhetoric of the most active participants in the IIS negotiation process in order to understand the prospects for the development of an international regime in the field of information security.

As shown in the first two chapters, the current state of affairs determines the high role of epistemic communities at the stage of shaping the agenda of international cooperation. Within the framework of the nuclear arms control regime, such a role was played by the Pugwash

[85] Robert Fanelli, "Cyberspace Offense and Defense." *Journal of Information Warfare* 15, no. 2 (2016): 53-65.

[86] Ben Azvine and Andy Jones. "Meeting the Future Challenges in Cyber Security." *In Industry 4.0 and Engineering for a Sustainable Future*, (Springer, Cham, 2019): 37-152.

[87] Joseph Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (2011): 24-25.

[88] Eric Jardine, "Taking the Growth of the Internet Seriously When Measuring Cybersecurity." *Researching Internet Governance: Methods, Frameworks, Futures* (2020).

Committee,[89] which took part in setting the agenda and the main formats of international cooperation. As representatives of the constructivist paradigm note,[90] in international politics, not only material factors, but also intersubjective ideas transmitted in the process of socialization (learning) are significant. The socialization process takes place on the basis of new knowledge, training and experience gained and gradually changes the perception of national interests and transforms the foreign policy course. Ongoing debates at the GGE and OEWG are analogous to those of the United States and the USSR several decades ago, when these countries had to reconsider their interests after realizing the mutual vulnerability and acknowledging the possibility and expediency of international cooperation. It is indicative that the Moscow-Washington hotline, created after the Cuban missile crisis, is now used for prompt warning of cyber incidents.[91]

However, negotiations on the establishment of an international nuclear arms control regime began only in the third decade after the creation of the atomic bomb. The first formal document was the 1963 Partial Nuclear Test Ban Treaty,[92] which was more environmental than military in nature. In addition, nuclear tests in the atmosphere were easy to verify, simplifying the task of monitoring the implementation of this agreement. The next significant agreement was the Treaty on the Non-Proliferation of Nuclear Weapons, which limited the spread of nuclear weapons to third countries. And the most developed mechanism was the START I Treaty, which set itself the task of controlling the number of nuclear weapons in the USSR and the United States and assumed the formation of a complex regime of mutual inspections, necessary in conditions of mutual distrust.

[89] Doubravka Olšáková, "Pugwash in Eastern Europe: The limits of international cooperation under Soviet control in the 1950s and 1960s." *Journal of Cold War Studies* 20, no. 1 (2018): 210-240.

[90] Alastair Iain Johnston, "Treating International Institutions as Social Environments." *International Studies Quarterly 45*, no. 4 (2001): 492.

[91] Joint statement by the Presidents of the United States of America and Russia on a new field of cooperation in confidence building, June 17, 2013.

[92] *Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water*, Moscow, 5 August 1963.

Similar to ICT, nuclear technology has spawned new dimensions in the relationship between civil and military spheres. Initially, nuclear energy was studied for military use, however, it soon became clear that it could be used for peaceful purposes.[93] In these conditions, the IAEA was created, the main purpose of which was to control the civilian use of nuclear technology. However, as researchers note,[94] US foreign policy strategy in this area was not limited solely to national interests. The activities of the IAEA were influenced by commercial structures, including the US government, who were interested in spreading new technology around the world in order to create a new market. The private sector also plays a significant role in the development of the information sphere, influencing the policy of states in this area and can also form the norms, principles and procedures for making decisions within the international regime.[95]

The progress of the negotiation process on the Comprehensive Nuclear Test Ban Treaty (CTBT) is also of relevance. While initially negotiations on a ban on nuclear tests were conducted between the "great powers", small states soon started to exert pressure on the position of the nuclear powers in alliances, appealing to the commitments undertaken earlier.[96] Although it is unlikely that the treaty will enter into force in the near future, the participating states are in no hurry to withdraw from it, which is due to the fact that this document has a significant psychological effect in world politics and violation of its provisions is perceived as a foreign policy problem. The experience of the negotiation process on the CTBT, which has not yet entered the phase of formal implementation, shows that in conditions when the stakes of the main participants in the negotiation process are high (refusal to test actually means the impossibility of improving and developing the nuclear potential, and also creates questions

[93] Rebecca Davis Gibbons, "The Humanitarian Turn in Nuclear Disarmament and the Treaty on the Prohibition of Nuclear Weapons." *The Nonproliferation Review* 25, no. 1-2 (2018): 11-36.

[94] Maria Rentetzi, "With Strings Attached: Gift-Giving to the International Atomic Energy Agency and US Foreign Policy." *Endeavour (New series)* 45, no. 1-2 (2021): 1-8.

[95] Henry Farrell, *Promoting Norms for Cyberspace*. (New York: Council on Foreign Relations, 2015).

[96] Maurice A. Mallin, "*The Comprehensive Nuclear-Test-Ban Treaty Negotiations : a Case Study*" (Washington, D.C: National Defence University Press, 2017).

regarding the reliability and safety of existing nuclear warheads) the negotiation phase of cooperation can last as long as desired, while informal rules of interaction are developed, although they do not impose obligations on the participants in the regime.

The main difficulty in using the experience of nuclear arms control lies in the specificity of ICTs. In the information sphere, in contrast to the nuclear sphere, it is not only difficult to trace the source of an attack but to also accurately assess its destructive potential. To ensure IIS, even closer international cooperation is required to create an atmosphere of trust, which complicates the negotiation process in this area. In these conditions a situation has developed that is conducive to the formation of an international legal regime for the non-proliferation of cyber weapons. It seems that a comprehensive IIS regime should imply the establishment of restrictions on the spread of any weapons that influence critical infrastructure systems as part of the international arms control system as a whole. On this basis it is advisable to rely on the experience of international agreements in the field of limiting or prohibiting weapons of mass destruction, as well as the Ottawa Convention on the Prohibition of the Use, Stockpiling and Production, Transfer and Use of Antipersonnel Mines of 1997.[97] However, ICTs are significantly more affordable than nuclear weapons. Thus, tracing the transfer of relevant technologies appears to be a daunting task. Control measures have made some progress in slowing the proliferation of nuclear technology and materials, while such results are difficult to achieve with respect to ICTs. This issue could be related to the relative advantage of a first strike. In a nuclear arms race, the threat of a disabling first strike has always been offset by the prospect of a potential retaliatory strike. This circumstance formed the basis of the well-known doctrine of "mutual assured destruction". In cyberspace, the first strike can be faster than a nuclear one, and as the identification of the source of the attack is difficult, the implementation of a containment policy is problematic.

[97] *Convention on the Prohibition of the Use, Stockpiling and Production, Transfer and Use of Antipersonnel Mines*, Ottawa, 3 December 1997.

Despite individual critics such as Martin Libicki,[98] most scholars agree on the effectiveness of a deterrent-based foreign policy in cyberspace.[99] However, for the effective implementation of such a policy, as the experience of the development of the nuclear security regime shows, an international crisis is needed. In this case, a balance of terror is established, and the Hobbesian culture of international interaction based on fear is transformed into a Grotian culture based on rivalry.

3.2 The International Legal Regime on Remote Sensing of the Earth from Outer Space

The extensive and large-scale development of ICTs provide ample opportunities in the field of remote sensing[100] of the Earth from Outer Space. In particular, by using such technology it is possible to monitor compliance with international agreements on the limitation of strategic weapons and address other issues of defense and security of states. Currently, more than 50 countries have their own remote sensing space systems,[101] and the total number of relevant satellites operating is more than 1000.[102] However, what currently governs relations in this important area of information and space technology?

The fundamental international legal basis for remote sensing is the 1967 Outer Space Treaty,[103] according to which all space activities are carried out for the benefit and in the interests of all countries, regardless of their level of economic or scientific development. Additionally, space activities are carried out by all states in accordance with international law, including the

---

[98] Martin Libicki, *Cyberdeterrence and Cyberwar*, (RAND corporation, 2009).

[99] Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (2012): 148-170.

[100] In general, it is the observation of the Earth, carried out from the most advantageous positions in outer space using the properties of electromagnetic waves that are emitted, reflected or scattered by probed objects. Cameras mounted on automatic remote sensing satellites, as well as on board spacecraft and orbital space stations, receive high-resolution images of the Earth's surface, the oceans and the Earth's atmosphere.

[101] Charles Toth and Grzegorz Jóźków, "Remote sensing platforms and sensors: A survey." *ISPRS Journal of Photogrammetry and Remote Sensing* 115 (2016): 22-36.

[102] UCS Satellite Database.

[103] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967.

UN Charter, without any discrimination, on the basis of equality and with free access to all areas of celestial bodies. Thus, it is the states that are internationally responsible for remote sensing, whether carried out by governmental or non-governmental legal entities.

In the first years of the space age, remote sensing was not subject to any additional special regulation. The need for it was for the first time discussed in 1971 by the UN Committee on the Peaceful Uses of Outer Space and resulted in the establishment of a working group which began to develop an international instrument to regulate relevant activities.[104] Initially, it was planned to develop a special treaty on remote sensing. However, it soon became clear that a formal legally binding agreement in this area would be a premature and unviable idea. Considering the rapid development of technology, it would have been virtually impossible to quickly adjust the "hard law", given the cumbersome procedure for such changes. The main problem that arose at that time which did not find an adequate solution was the issue of the balance between the sovereignty of the probed states with the principle of freedom of space activities in relation to remote sensing.[105] The negotiations were dominated by two opposing positions: states that had previously engaged in remote sensing considered that these activities did not require any reservations compared to the general principles and norms of international space law i.e. it was sufficient to codify the rules already in place at that time; other states (primarily a group of developing countries that did not carry out their respective activities on their own) fought for the need to regulate compliance with national sovereignty during remote sensing.[106]

[104] United Nations, General Assembly, *Convening of the Working Group on Remote Sensing of the Earth by Satellites*, A/RES/2778(XXVI) (29 November 2017).

[105] Philippe Achilléas, *Droit de l'espace: télécommunication, observation, navigation, défense, exploration*. (Bruxelles: Larcier 2009): 144.

[106] Carl Quimby Christol, *Space Law: Past, Present, and Future* (The Netherlands: Kluwer Law and Taxation Publishers 1991): 90-95.

After fifteen years of work on the convergence of positions, 15 legal principles were developed, adopted by consensus by UN General Assembly Resolution 41/65.[107] It should be noted here that not all UN resolutions are equal. Declarations of principles have high moral and political potential, so they cannot be ignored by states, especially if they have been adopted by consensus.[108] Some scholars,[109] referring to the authority of the UN on whose behalf such declarations of principles are adopted, as well as to the will of members of the international community who have agreed with them, even consider these acts to be implemented by states as a result of international custom. Nonetheless, Resolution 41/65 only considers remote sensing "for the purpose of improving national resources management, land use and the protection of the environment".[110] Thus, not only does it not include many types of civilian remote sensing, such as activities carried out for meteorological purposes, it completely ignores military applications. As a result, the legal regime for the regulation of remote sensing activities for security and defense purposes is currently governed by the international treaties on disarmament and arms control, rather than these Principles. In addition, at present, remote sensing space missions often combine civilian and military purposes; hence it is also not clear under which legal regime such missions fall.

The challenges faced by the international legal regime on remote sensing of the Earth from Outer Space are in many ways similar to the challenges that stand in the way of international cooperation in ensuring information security:

1. Militarization - a growing number of states can simultaneously use technology for both civilian and military purposes.

[107] General Assembly resolution 41/65, *Principles relating to remote sensing of the Earth from outer space*, A/RES/41/65 (3 December 1986).

[108] Joanne Irene Gabrynowicz, "Defining Data Availability for Commercial Remote Sensing Systems Under United States Federal Law." *Annals of air and space law* 23 (1998): 95-96. Vladimir Kopal, "The Role of United Nations Declarations of Principles in the Progressive Development of Space Law." *Journal of Space Law* 16, no. 1 (1988): 16.

[109] Stephen Schwebel. "The Effect of Resolutions of the U.N. General Assembly on Customary International Law." *Proceedings of the annual meeting - American Society of International Law* 73 (1979): 301–309.

[110] According to Principle 1 in the Annex of General Assembly resolution 41/65.

2. Privatization - the number of private initiatives in the space sector is growing, therefore, the influence of non-state actors that do not participate in the international regime is increasing.[111] Moreover, the regulation of Big Tech Companies and the Internet itself is underdeveloped. [112]

In the both high-tech areas reviewed, there is a phenomenon of world politics that can be designated as "technological isomorphism" - the similarity of models of international political interaction and cooperation regarding the regulation of the field of world politics arising in connection with the development of new technologies manifests itself at different stages of maturity of these technologies. At the initial stages of technology development, the role of the expert community (also called the epistemic community) is strong. At subsequent stages, the state and the private sector increase their influence. A necessary condition for the development of international cooperation is the recognition of a common vulnerability, and international crises contribute to the transition of negotiation to the stage of implementation of agreements. There is a mutual influence of technology and world politics, although ICTs are often inscribed in a broader social and political context. The nature of their regulation reflects the features of the international system, the political model of the world, based on Westphalian principles and in this regard is conservative, which explains the phenomenon of isomorphism.

At the same time, "technological isomorphism" is not absolute, differences should also be noted. Firstly, they affect the nature of the technology and the different directions of its use. Secondly, while the nuclear arms control regime and the international legal regime of remote sensing were formed during the period of the stable bipolar system of the Cold War and therefore are global in nature, then with regard to information security in the absence of consensus between the major powers and an unsettled system of a "balance of terror" we are

[111] Natalie Bormann and Michael Sheehan, eds. *Securing Outer Space: International Relations Theory and the Politics of Space* (Routledge, 2009): 2.

[112] Sara M. Smyth, "The Facebook Conundrum: Is it Time to Usher in a New Era of Regulation for Big Tech?." *International Journal of Cyber Criminology* 13, no. 2 (2019): 578-595.

only witnessing the formation of several regional regimes. This reflects on the one hand, the specifics of ICT as an object of regulation at the international level, and on the other hand, the trend towards regionalization of world politics and, as a consequence, the information space, discussed in the second chapter of this thesis.

3.3 Prospects for Achieving a Global Consensus on Information Security

As Robert Jervis, an American scholar in the theory of international relations, argues,[113] the formation of regimes in the field of security is more difficult than in the economic sphere, due to the inherent competitive nature of most security problems (and competition is often irreconcilable), as well as the difficulty in determining the necessary level for survival. The experience of the nuclear arms control regime and remote sensing confirms the possibility of forming regimes characterized by principles, norms and decision-making procedures. According to Jervis, a regime will only be sustainable (will function for a long time and effectively prevent conflicts between its members) if the basic norms are internalized, that is, the constraints inherent in the regime and based on the norms and principles that underlie it are internal in nature and are part of the identity of states, are perceived by them as an integral part of foreign policy ideology.

At first glance, there are two main approaches to the legal regulation of IIS:

The first approach can be described as "real" law.[114] It is based on the assumption that modern ICT does not have a qualitatively different specificity in comparison with the technology that preceded it. It is undeniably faster than its predecessors, however, this does not mean that it has a new quality that requires new rules and regulations. Therefore, all existing relevant legal frameworks can be used unchanged to regulate IIS.

[113] Robert Jervis, "Security Regimes." *International Organization* 36, no. 2 (1982): 357–378.

[114] A law is real if the subject of the law has the practical ability to exercise its rights.

The second approach, on the contrary, proceeds from the assumption that modern ICT is still a qualitatively new phenomenon, for which it is necessary to develop new norms and rules - "cyber law".[115] The main argument of the proponents of this approach is the indication of the unprecedented speed of data transmission over the Internet, as well as the network (and not hierarchical) nature of the organization of ICT infrastructure.

In practice, such approaches are a reflection of the real political interests of states. The problem of adapting international law to the information sphere is highly politicized and the qualitative specificity of ensuring information security at the global level in the long run depends on what legal principles the regulation of the global information space will be based on. The Internet, the global information space formed on its basis, and other modern ICTs, have a number of specific characteristics that complicate the applicability of the existing body of international law to this area. The existing corpus of international humanitarian law is applicable to the information sphere only if it is substantially adapted. In this regard, particularly significant is the problem of international legal regulation of the use of information weapons against objects of critical information infrastructure. Information warfare differs in many respects from the confrontation between states in the "real" world. Many of the provisions of international humanitarian law were developed in relation to the conventional means of warfare and in modern conditions need to be improved. Nonetheless, universally recognized principles of international law *jus cogens*, the UN Charter (namely, non-interference in the internal affairs of states and the non-use of force and the threat of force), must remain unshakable both in the traditional, physical, and in the new, digital space.

Ultimately, it is only feasible to study the issue of applicability and sufficiency of international law to the field of IIS if the existence and possibility of using ICTs as weapons is acknowledged, and an organized confrontation with their use is recognized as war. As shown in

[115] Miograd N. Simovic, Zivorad Rasevic, and Vladimir M. Simovic, "Cyber Warfare and International Cyber Law: Whither?." *Journal of Criminology and Criminal Law* 58 (2020): 23.

this thesis, the international community is slowly coming to this understanding. Countries tend to recognize their vulnerabilities and are willing to adopt international legal documents that regulate and restrict the possibility of aggressive actions in the infosphere. In this regard, the United States and its NATO partners, on the one hand, and Russia+China and their partners in the SCO and BRICS, on the other, act as norm entrepreneurs,[116] offering their vision of the legal regulation of the global information space in general and the sphere of IIS in particular. According to Martha Finnemore's theory of international norms, their development will go through several stages - the advancement of norms by norm entrepreneurs, cascading distribution and then internalization. Currently, the development of international norms governing the global information space is only at the first stage. Thus, without an agreement on the norms of interaction in the field of IIS, further development of international cooperation in this area at the global level is impossible.

[116] Finnemore, "Norm Dynamics and Political Change," 893.

Conclusion

There are two competing securitizing discourses in the field of ensuring IIS that have developed in international law. The "cybersecurity" discourse implies that exclusively technological aspects of information security are subject to regulation at the international level, while the "information security" discourse involves ensuring not only the technical security of information networks and systems, but also a wider range of issues related to content regulation in in order to ensure social stability. The United States, EU and NATO promotes the discourse of "cybersecurity", while Russia and China, as well as partner states of these countries in such organizations as SCO, BRICS, support the discourse of "information security".

Trends in the development of the international system, in particular, the increasing conflict in relations between major powers and regionalization,[117] have an impact on the information sphere. This new "Digital Westphalia" (similar to the Westphalian Peace Treaty, following which the principle of state sovereignty formed the basis of international relations in Europe and then throughout the world) involves strengthening state sovereignty and a trend towards multipolarity in the information sphere.[118]

States are key actors in ensuring international information security. Non-state actors are inferior to states in terms of their influence. The global information sphere is conceptualized by most states as an arena of interstate confrontation and conflict and is thus a securitized area of world politics. Despite the significance of terrorist and criminal threats, the most important threat to international information security is the use of ICT by states for military-political purposes, moreover, its use in the absence of developed international rules of conduct can destabilize the international security system as a whole.

---

[117] Mearsheimer, *Great Power Politics*.

[118] Brandon Valeriano and Ryan C. Maness, "International Relations Theory and Cyber Security." *The Oxford Handbook of International Political Theory* (2018): 259-275.

Due to the high importance of information security and the lack of a balance of threats (which is influenced by the specificity of ICT), international cooperation is still at the stage of negotiated bargaining and has not yet moved to the stage of implementation of agreements. There is no single global information security regime. Rather, one can observe a set of disparate initiatives and regimes, both regional and bilateral, aimed at solving specific security problems arising in the "digital age", which to a certain extent reflects the trend of regionalization in world politics and the information space. The negotiation process at the global level masks the arms race in the information space.

International cooperation in ensuring information security does not differ significantly from the models of cooperation that have developed in other reviewed areas of world politics. Thus, the argument of the thesis was confirmed, according to which the nature of international cooperation depends, first of all, not on the technological characteristics of the particular area in which cooperation is conducted, but on the nature of relations between key actors and the perception of their interests.

The negotiation process on information security will continue until an acute international crisis establishes a balance of terror between the parties and international cooperation moves to the implementation phase, which, given the importance of this issue, promises to be effective. The analysis of international cooperation in the field of nuclear arms control speaks in favor of such an assertion.

In the short term, the global information security regime will develop similarly to the legal regime of remote sensing of the Earth from Outer Space. The basis for such a regime can be the principles and norms of behavior of states in the information sphere, agreed at the universal level. However, the growing complexity of information technology in the long term may lead to the formation of a "tougher" international regime in many ways similar to the nuclear arms control regime.

In terms of future research, it is evident that the experience of domestic regulation should be used in the development of international legal norms. In many parts of the world, elements of the national critical infrastructure are owned by the private sector and are not fully controlled by the state. As such, it is important to study the system of their effective protection through the prism of international law.

Bibliography

Achilléas, Philippe. *Droit de l'espace: télécommunication, observation, navigation, défense, exploration*. Bruxelles: Larcier 2009.

African Union, *African Union Convention on Cyber Security and Personal Data Protection*, 27 June, 2014.

Akdag, Yavuz. "The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective." *Journal of Chinese Political* Science 24, no. 2 (2019): 225-247.

Al Izki, Fathiya, and George Weir, "Information security and digital divide in the Arab world." *In Cyberforensics 2014-International Conference on Cybercrime, Security & Digital Forensics* (2014): 15-24.

Azvine, Ben, and Andy Jones. "Meeting the Future Challenges in Cyber Security." *In Industry 4.0 and Engineering for a Sustainable Future*, (Springer, Cham, 2019): 37-152.

Belli, Luca. *CyberBRICS : Cybersecurity Regulations in the BRICS Countries*. Cham, Switzerland: Springer, 2021.

Bolgov, Radomir. "The UN and Cybersecurity Policy of Latin American Countries." *In 2020 Seventh International Conference on eDemocracy & eGovernment* (ICEDEG, 2020): 259-263.

Bormann, Natalie, and Michael Sheehan, eds. *Securing Outer Space: International Relations Theory and the Politics of Space*. Routledge, 2009.

Budnitsky, Stanislav, and Jia Lianrui. "Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance." *European Journal of Cultural Studies* 21, no. 5 (2018): 594-613.

Busch, Marc L. "Overlapping institutions, forum shopping, and dispute settlement in international trade." *International Organization* (2007): 735-761.

Castells, Manuel. "Communication, power and counter-power in the network society," *International Journal of Communication* 1, no. 1 (2007): 238-266.

Center for Strategic and International Studies. *Significant Cyber Incidents*. May 24, 2021.

Chadwick, Andrew, and Philip N. Howard. *Routledge Handbook of Internet Politics*. London: Routledge, 2009.

Choucri, Nazli, Stuart Madnick and Jeremy Ferwerda, "Institutions for cyber security: International responses and global imperatives." *Information Technology for Development* 20, no. 2 (2014): 96-121.

Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, Mass: MIT Press, 2012.

Christol, Carl Quimby. *Space Law : Past, Present, and Future*. The Netherlands: Kluwer Law and Taxation Publishers, 1991.

Cogburn, Derrick L. "Relinquishing the Root: Snowden, NETmundial, and the IANA Transition." *In Transnational Advocacy Networks in the Information Society*, (Palgrave Macmillan, New York, 2017): 247-262.

Commonwealth of Independent States. *Agreement on Cooperation in Combating Offences related to Computer Information*, June 1, 2001.

Convention on the Prohibition of the Use, Stockpiling and Production, Transfer and Use of Antipersonnel Mines, Ottawa, 3 December, 1997.

Council of Europe, *Convention on Cybercrime*, 23 November, 2001.

Deibert, Ronald. "Trajectories for Future Cybersecurity Research." *In The Oxford Handbook of International Security* (2018): 531-556.

Eriksson, Johan, and Giampiero Giacomello, eds. *International Relations and Security in the Digital Age*. Vol. 52. Routledge, 2007.

European Commission. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade, Brussels*, 16 December 2020.

European Union. *Directive on Security of Network and Information Systems (NIS Directive)*, 6 July, 2016.

Fanelli, Robert. "Cyberspace Offense and Defense." *Journal of Information Warfare* 15, no. 2 (2016): 53-65.

Farrell, Henry. Promoting Norms for Cyberspace. *Council on Foreign Relations*, 2015.

Fearon, James D. "Bargaining, Enforcement, and International Cooperation." *International Organization* 52, no. 2 (1998): 269-305.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.

Finnemore, Martha. "Cultivating International Cyber Norms." *America's Cyber Future: Security and Prosperity in the Information Age* 2 (2011): 87-102.

France Diplomatie. *Paris Call for Trust and Security in Cyberspace*, 12 November, 2018.

Gabrynowicz, Joanne Irene. "Defining Data Availability for Commercial Remote Sensing Systems Under United States Federal Law." *Annals of Air and Space Law* 23 (1998): 95-96.

Gamreklidze, Ellada. "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia." *Journal of International Communication* 20, no. 2 (2014): 200–217.

General Assembly resolution 41/65, *Principles relating to remote sensing of the Earth from outer space*, A/RES/41/65 (3 December 1986).

General Assembly resolution 45/109, *Computerization of criminal justice*, A/RES/45/109 (14 December 1990).

General Assembly resolution 45/121, *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, A/RES/45/121 (14 December 1990).

General Assembly resolution 53/73, *Role of science and technology in the context of international security and disarmament*, A/RES/53/73 (4 January 1999).

General Assembly resolution 54/49, *Developments in the field of information and telecommunications in the context of international security*, A/RES/54/49 (23 December 1999).

General Assembly resolution 56/183, *World Summit on the Information Society*, A/RES/56/183 (31 January 2002).

General Assembly resolution 58/32, *Developments in the field of information and telecommunications in the context of international security*, A/RES/58/32 (8 December 2003).

General Assembly resolution 69/28, *Developments in the field of information and telecommunications in the context of international security*, A/RES/69/28 (2 December 2014).

General Assembly resolution 73/27, *Developments in the field of information and telecommunications in the context of international security*, A/RES/73/27 (5 December 2018).

General Assembly resolution 75/240, *Developments in the field of information and telecommunications in the context of international security*, A/RES/75/240 (31 December 2020).

Gerring, John. *Case Study Research : Principles and Practices*. New York: Cambridge University Press, 2007.

Gibbons, Rebecca Davis. "The humanitarian turn in nuclear disarmament and the treaty on the prohibition of nuclear weapons." *The Nonproliferation Review* 25, no. 1-2 (2018): 11-36.

Giles, Keir, and William Hagestad. "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." *In 2013 5th International Conference on Cyber Conflict* (CYCON 2013): 1-17.

Gorr, David, and Wolf J Schünemann. "Creating a Secure Cyberspace – Securitization in Internet Governance Discourses and Dispositives in Germany and Russia". *The International Review of Information Ethics* 20 (Edmonton, Canada 2013): 37-51.

Government of the Russian Federation. *On the signing of an Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security*, Moscow, 30 April 2015, https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf.

Grieco, Joseph M. "Anarchy and the Limits of Cooperation: a Realist Critique of the Newest Liberal Institutionalism." *International Organization* 42, no. 3 (1988): 485-507.

Healey, Jason, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd, "Confidence-building measures in cyberspace." *Atlantic Council, Brent Scowcroft Center on International Security* (2014).

Hill, Steven. "NATO and the International Law of Cyber Defence." *Research Handbook on International Law and Cyberspace (2nd edition)*(2020 Forthcoming) (2020): 1-15.

Jardine, Eric. "Taking the Growth of the Internet Seriously When Measuring Cybersecurity." *Researching Internet Governance: Methods, Frameworks, Futures* (2020).

Jervis, Robert. "Security Regimes." *International Organization* 36, no. 2 (1982): 357–378.

Johnston, Alastair Iain. "Treating International Institutions as Social Environments." *International Studies* Quarterly 45, no. 4 (2001): 487-515.

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 of the European Commission and Higher Representative for foreign affairs and security policy. Brussels (2013).

Joint statement by the Presidents of the United States of America and Russia on a new field of cooperation in confidence building, June 17, 2013.

Kaska, Kadri, Henrik Beckvard and Tomas Minarik, "Huawei, 5G and China as a security threat." *NATO Cooperative Cyber Defense Center for Excellence* (CCDCOE, 2019).

Kearn, David. "The Baruch Plan and the Quest for Atomic Disarmament." *Diplomacy & Statecraft* 21, no. 1 (2010): 41-67.

Kopal, Vladimir. "The Role of United Nations Declarations of Principles in the Progressive Development of Space Law." *Journal of Space Law* 16, no. 1 (1988): 16.

Kratochwil, Friedrich V. *Rules, Norms, and Decisions : on the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*. Cambridge University Press, 1991.

Kubiak, Katarzyna. "Towards a More Stable NATO-Russia Relationship." *European Leadership Network* (2019).

League of Arab States. *Arab Convention on Combating Information Technology Offences*, 21 December, 2010.

Lewis, James. "Confidence-building and international agreement in cybersecurity." *Disarmament Forum* 4 (2011): 51-59.

Liaropoulos, Andrew. "Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?" *Journal of Information Warfare* 12, no. 2 (2013): 19-26.

Libicki, Martin C. "Is There a Cybersecurity Dilemma?" *The Cyber Defense Review* 1, no. 1 (2016): 129-140.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*, RAND corporation, 2009.

Lieberthal, Kenneth, and Peter Warren Singer. *Cybersecurity and US-China relations*, (Brookings, 2012).

Mačák, Kubo. "From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers." *Leiden Journal of International Law* 30, no. 4 (2017): 877–899.

MacKenzie, Paul J. "NATO's Vision and Strategy on the Cyberspace Domain", *Journal of the Japcc*, no 28 (2019): 16-22.

Mallin, Maurice A. "The Comprehensive Nuclear-Test-Ban Treaty Negotiations : a Case Study" (Washington, D.C: National Defence University Press, 2017).

Mearsheimer, John. *The Tragedy of Great Power Politics*. WW Norton & Company, 2001.

Millennium Declaration, Millennium Summit of the United Nations New York, 6-8 September 2000.

Milner, Helen. "International Theories of Cooperation among Nations: Strengths and Weaknesses." *World Politics* 44, no. 3 (1992): 466-496.

Ministry of Foreign Affairs of the People's Republic of China. *International Strategy of Cooperation on Cyberspace*. Beijing, 2017.

Neuneck, Görz. "Civilian and Military Cyberthreats: Shifting Identities an Attribution." *The Cyber Index. International Security Trends and Realities*. (UNIDIR, 2013).

Nye, Joseph. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (2016): 44-71.

Nye, Joseph. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (2011): 18-25.

Nye, Joseph. "The Regime Complex for Managing Global Cyber Activities", Vol. 1. *Belfer Center for Science and International Affairs*, (John F. Kennedy School of Government, Harvard University, 2014).

Olšáková, Doubravka. "Pugwash in Eastern Europe: The limits of international cooperation under Soviet control in the 1950s and 1960s." *Journal of Cold War Studies* 20, no. 1 (2018): 210-240.

Panke, Diana. "Lock-in Strategies in International Negotiations: The Deconstruction of Bargaining Power." *Millennium* 43, no. 2 (2015): 375–391.

Paulsen, Celia, and Robert Byers. Glossary of key information security terms. NIST Internal or Interagency Report (NISTIR) 7298 Rev. 3. *National Institute of Standards and Technology*, 2019.

Pohle, Julia, and Thorsten Thiel. "Digital sovereignty". *Internet Policy Review* 9, no. 4 (2020): 1-19.

Rentetzi, Maria. "With Strings Attached: Gift-Giving to the International Atomic Energy Agency and US Foreign Policy." *Endeavour (New series)* 45, no. 1-2 (2021): 1-8.

Risen, Tom. "China, Russia Seek New Internet World Order." *US News and World Report* 14 (2015).

Rosato, Sebastian. "The Inscrutable Intentions of Great Powers." *International Security* 39, no. 3 (2015): 48–88.

Schjolberg, Stein, and Solange Ghernaouti-Helie. "A Global Treaty on Cybersecurity and Cybercrime." *Cybercrime Law* 97 (2011),

https://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf

Schmitt, Michael N. ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013.

Schmitt, Michael N., and Liis Vihul, "Proxy Wars in Cyber Space: The Evolving International Law of Attribution," *Fletcher Security Review* 55-73 (2014): 19.

Schwebel, Stephen. "The Effect of Resolutions of the U.N. General Assembly on Customary International Law." *Proceedings of the annual meeting - American Society of International Law* 73 (1979): 301–309.

Shanghai Cooperation Organisation. *Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security*, Yekaterinburg, 16 June 2009.

Simovic, Miodrag N., Zivorad Rasevic, and Vladimir M. Simovic. "Cyber Warfare and International Cyber Law: Whither?." *Journal of Criminology and Criminal Law* 58 (2020): 23.

Smeets, Max. "Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment." *Defence Studies* 18, no. 4 (2018): 395-410.

Smyth, Sara M. "The Facebook Conundrum: Is it Time to Usher in a New Era of Regulation for Big Tech?." *International Journal of Cyber Criminology* 13, no. 2 (2019): 578-595.

Soesanto, Stefan, and Fosca D'Incau. "The UN GGE Is Dead: Time to Fall Forward," *European Council on Foreign Relations*, August 15, 2017, https://ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance/

Stevens, Tim. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33, no. 1 (2012): 148-170.

Sullivan, Julia E., and Dmitriy Kamensky. "How Cyber-attacks in Ukraine show the Vulnerability of the US power grid." *The Electricity Journal* 30, no. 3 (2017): 30-35.

The Department of Defense Cyber Strategy, Washington, April 2015.

The Ministry of Foreign Affairs of the Russian Federation, *CONVENTION ON INTERNATIONAL INFORMATION SECURITY (Concept)*, 22 September 2011.

The Okinawa Charter on the Global Information Society, Kyushu-Okinawa Summit 2000, 23 July 2000.

Toffler, Alvin. *Powershift : Knowledge, Wealth, and Violence in the 21st Century*. New York: Bantam Books, 1990.

Toth, Charles, and Grzegorz Jóźków. "Remote sensing platforms and sensors: A survey." *ISPRS Journal of Photogrammetry and Remote* Sensing 115 (2016): 22-36.

Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, Moscow, 5 August 1963.

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 27 January 1967.

UCS Satellite Database.

United Nations, General Assembly, *Convening of the Working Group on Remote Sensing of the Earth by Satellites*, A/RES/2778(XXVI) (29 November 2017).

United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General*, A/70/174 (22 July 2015).

United Nations, General Assembly, *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*, A/69/723 (13 January 2015).

United Nations, *Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, A/CONF.187/15 (10-17 April 2000).

Valeriano, Brandon, and Ryan C. Maness. "International Relations Theory and Cyber Security." *The Oxford Handbook of International Political Theory* (2018): 259-275.

Von Solms, Rossouw, and Johan Van Niekerk, "From Information Security to Cyber Security." *Computers & security* 38 (2013): 97-102.

Wendt, Alexander. *Social Theory of International Politics*. Cambridge, UK : Cambridge University Press, 1999.

Wirth, Axel. ""The Cyber Arms Race Is On': Lessons from the U.S. Presidential Election." *Biomedical Instrumentation & Technology* 50, no. 6 (2016): 463–465.

Wolfers, Arnold. ""National security" as an Ambiguous Symbol." *Political science quarterly* 67, no. 4 (1952): 481-502.

Young, Oran R. *International Cooperation : Building Regimes for Natural Resources and the Environment*. Ithaca: Cornell University Press, 1989.