RESEARCH PROJECT
INTERNATIONAL INFORMATION
SECURITY RESEARCH CONSORTIUM

METHODOLOGICAL ISSUES OF THE APPLICATION OF NORMS, RULES AND PRINCIPLES OF RESPONSIBLE BEHAVIOUR OF STATES TO PROMOTE AN OPEN, SECURE, STABLE, ACCESSIBLE AND PEACEFUL ICT ENVIRONMENT

Edited by
Prof Anatoly A. Streltsov
Dr. Eneken Tikk

RESEARCH PROJECT
INTERNATIONAL INFORMATION SECURITY RESEARCH CONSORTIUM

METHODOLOGICAL ISSUES OF THE APPLICATION OF NORMS, RULES AND PRINCIPLES OF RESPONSIBLE BEHAVIOUR OF STATES TO PROMOTE AN OPEN, SECURE, STABLE, ACCESSIBLE AND PEACEFUL ICT ENVIRONMENT

Edited by
Prof Anatoly A. Streltsov
Dr. Eneken Tikk

2020

PARTICIPANTS OF THE PROJECT

Anatoly Streltsov, Moscow State University, National association of international information security, Russian Federation

Valery Yaschenko, Moscow State University Russian Federation

Pavel Karasyev, Moscow State University, Russian Federation

Andreas Kuehn, EastWest Institute, United States of America

Vladimir Ivanov, EastWest Institute, United States of America

EnekenTikk, Cyber Policy Institute, Estonia

Mika Kerttunen, Cyber Policy Institute, Finland

Daniel Stauffacher, ICT4Peace Foundation, Switzerland

ISBN 978-5-6044056-2-8

CONTENTS

FOREWORD

The 2000 Okinawa Declaration on the Formation of a Global Information Society ushered in a new era in the development of mankind. This era is characterized by the intensive development of the global environment of information and communication technologies (ICT environment). This environment is made possible by the global information infrastructure. The ICT environment has acquired the features of a new space in international relations, which create new opportunities for improving the quality of human life, sustainable development of society, and for the emergence of international disputes that could lead to threat or breach of international peace and security. The threat of hostile use of ICTs for politico-military purposes is growing. The number of ways ICTs can be used to exert forcible effects on the adversary and other targets are constantly increasing.

The Russian Federation, like many other countries, has consistently advocated for the creation of an international information security system aimed at preventing the "hostile" use of ICTs as the means of resolving interstate conflicts. To this end, the Russian Federation initiated the formation of several groups of governmental experts on developments in the field of information and telecommunications in the context of international security. The practical usefulness of this initiative is now recognized by almost all states of the world.

The efforts of UN governmental experts, who in 2003 began to study the potential dangers to threats to international peace and security in the use of ICTs, were rewarded by the adoption of a consensus report to the UN Secretary General in 2010, 2013 and 2015. For the first time, the 2015 report contained recommendations on the norms, rules and principles of responsible behavior of states in ICT environment.

With the adoption at the 73rd session of the UN General Assembly of the draft Russian resolution, fixing the recommendations of the UN Group of Governmental Experts on the norms, principles and rules of responsible behavior of states in the ICT environment as the norms of "soft" law, the problem of ensuring the practical application of these norms becomes particularly relevant[1]. In the deteriorating international situation, experts from many countries of the world believe that the development of specific recommendations on the implementation of the norms, rules and principles of responsible behavior of states in the ICT environment could help reduce the risk of conflicts associated with the hostile and malicious use of ICTs by states in international relations.

There is no doubt that international relations in the ICT environment should be regulated by international law. However, countries are not united as to how and to what extent international law is applicable in the ICT environment.

In this regard, the initiative of the participants of the International Information Security Research Consortium (IISRC), put forward in April 2018 at the International Forum in Garmisch-Partenkirchen (Germany), to form an international group of experts to discuss methodological differences in, and develop common approaches for, assessing the applicability of norms, rules and principles of responsible behavior is extremely timely to contribute to an open, secure, stable, accessible and peaceful ICT environment. The group included experts from interested organizations in the Russian Federation, USA, Estonia, South Korea and Switzerland.

We are confident that the potential of Russian experts studying the problems of creating an international information security system and, in particular, the practical application of the norms, rules and principles of responsible behavior of states in the ICT environment, will increase significantly with the formation in 2018 of the National Association of International Information Security. One of the important activities of the Association is to proactively address the challenges of ensuring international information security. Based on this, the Association will make efforts to promote research into the problems of the practical application of the norms, prin-

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

ciples and rules of responsible behavior of states in the ICT environment, carried out within the framework of the project of the International Consortium.

I am pleased to offer the reader the materials of the study of an international group of experts on the results of its work in 2018–2019, which undoubtedly deserve thorough examination and further discussion.

President of the National Association of International Information Security

Chairman, International Information Security Research Consortium

Vladislav Sherstyuk

EXECUTIVE SUMMARY

At the request of the International Information Security Research Consortium, Moscow State University , represented by the Institute of Information Security Issues, in cooperation with Korea University, the ICT for Peace Foundation, Cyber Policy Institute and the EastWest Institute undertook a study of implementing the norms, rules and principles of responsible behaviour of States as developed by the 2014-2015 UN GGE and incorporated in Resolution A/73/27 of the UN General Assembly.

The UN GGE has concluded that these recommendations contribute to maintaining an open, secure, stable, accessible and peaceful ICT environment. Consequently, this study reviews the concepts of ICT environment, its distinct features and the desired characteristics of it. Importantly, this study examines the relationship between these recommendations, or norms, and international law, concluding that these recommendations, by way of their existence as well as their implementation, contribute to the development of international law. It fills into the gap that exists in the current discourse by promoting a methodological, rather than ideological, approach to the question of responsible State behaviour.

This study shows that the main actors in international information security, the United States and the Russian Federation do not necessarily disagree about the existence and importance of the key concepts and institutions, such as sovereignty, human rights or international law. The states do not agree with that, how exactly the opposite side applies these tools in the international relations.

Accordingly, this study offers a way to minimize the effect of such disagreements by demonstrating a methodological approach to developing common understanding and achieving universal implementation of the UN GGE recommendations. It provides a framework that can be applied to opening individual problems of international information/cyber security, examining the proposed solutions and their intended effect. Furthermore, this methodology emphasizes the maxim of international law in international information/cyber security. The study opens up the prospect of a productive discussion of specific rules, standards and other measures for the practical application of international law to the international relations under consideration.

The goal of the group of participants in this international project was to find a methodological approach for solving the problems of ensuring international information security (cybersecurity) by creating an open, safe, stable, accessible and peaceful ICT environment

Participants of the study have applied the proposed methodology on three distinct examples, recommendations in paragraph 13 (g), (h) and (k) of the UN GGE 2015 report. For each recommendation, the study offers views as to specific challenges related to its implementation.

I. INTRODUCTION

This study addresses the implementation of norms, rules and principles of responsible behaviour of States that contribute to maintaining an open, secure, stable, accessible and peaceful ICT environment[2]. In accordance with the decision of the International Information Security Research Consortium (2018, April 14, Garmisch-Partenkirchen), this study addresses paragraphs 13 (g), (h) and (k) of the (2015) *Report of the Group of Governmental UN experts (UN GGE) on developments in the field of information and telecommunications in the context of international security* (hereinafter also the GGE Report).

This study takes a particular methodological approach to assessing the applicability of international law to international relations in the ICT environment and formulating the problems of practical application by states of the norms, rules and principles of responsible behavior in the ICT environment. The study also offers views on the interpretation of the concept of "ICT environment" as an area for international cooperation.

The above interpretations assume that the voluntary, non-binding norms, rules and principles of responsible behavior of States in the ICT environment are implemented primarily on the basis of national legislation and within the framework of national jurisdiction. The study addresses the issues of practical application of the considered norms, rules and principles to international relations in the ICT environment.

The methodological approach taken in this study seeks to clarify the conditions under which a common opinion of experts can be formed on the application of the recommendations of the UN GGE, contributing to the creation of an open, safe, stable, peaceful and accessible ICT environment.

This material is directed at scholars and experts dealing with the issues of international and national information security (cybersecurity). The materials of the study can be used to ensure the effective use of the potential of the sovereignty of states in the ICT environment in line with the goals of sustainable development, and can inform developing international and national documents that determine relevant strategy and policy.

Participants of this study did not seek to produce a consensus report but rather to explore and expose the most critical issues and divergences hindering progress in the development and implementation of the norms, rules and principles of responsible State behavior in the ICT environment. Numerous statements in this material are followed by remarks outlining the differences in views and interpretations discovered in the course of the project discussions. Other statements, being ostensibly unanimous, may lead to further disagreements at deeper levels of detailed discussions. This pioneer research effort is considered by participants as a starting point for multidisciplinary process involving scientists and practitioners of diverse horizons, starting with cyber and information security strategy planners and investigators, policy developers, lawyers, diplomats and ICT operators.

The study allows to discuss factors that have caused sharp differences in the positions of States on the application of the norms, principles and rules of responsible behavior of states in the ICT environment. It also addresses priority areas for the development of these norms, principles and rules in order to create an open, safe, stable, peaceful and accessible ICT environment.

Currently, experts' positions diverge significantly in matters of assessing the possibility of applying international law to regulate international relations in the ICT environment. This will inevitably affect the ways of implementing the recommendations of the UN GGE and the effectiveness of their practical application. It is hoped that the study of difficulties in understanding the subject matter of legal regulation and objective difficulties in applying international law to international relations in the ICT environment can help to strengthen mutual

2 In this study, the ICT environment refers to a emerging set of national, international and global ICT systems used to provide services and host information systems. At the same time, in the context of a possible subsequent study of the application of the principle of "non-interference in the internal affairs of other states" to international relations in the ICT environment it is important to note that ICTs are not only a means of creating information systems, but are also actively used to automate the formation and distribution of content to consumers.

understanding and create an atmosphere of trust between states in this new area of international relations.

From this point of view, the materials of the study can contribute to inform the expert discussion in the field of international information security[3] (cybersecurity[4]) on preventing malicious and hostile use of ICTs, which can cause international friction and disputes, and threats to international peace and security.

3 Accorsing to the Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization (June 15, 2009), international information security is understood as the state of international relations, eliminating the violation of world stability and creating a threat to the security of states and the international community in the information space. Agreement between the governments of the member states of the Shanghai Cooperation Organization in the field of international information security. - http://base.garant.ru/2571379/

4 The US National Cyber Strategy outlines how the United States of America will (1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability — in concert with allies and partners — to deter and if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet. National Cyber Strategy of the United states of the America. September 2018.- https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

PART I

II. GENERAL FORMULATION OF THE RESEARCH PROBLEM AND THE NEED FOR A METHODICAL APPROACH

1. Intensive and wide use of ICTs in all spheres of public and private life has created conditions for, and led to, the formation and development of the global information society[5]. It is widely acknowledged that reliance and dependence on ICTs brings not only opportunities but also serious threats to national, and potentially international, security.

2. International security can be interpreted as a state of international relations, in which, on the basis of international law, the necessary conditions for the sustainable development of sovereign states and the individuals in the economic, social, political and cultural spheres are created, and the necessary level of environmental protection is maintained. The security of critical infrastructures and critical information infrastructures through the application of international law and through the exercise of national jurisdiction will contribute to sustainable development of the society.

3. To study threats in the field of information security and elaborate on international concepts of ensuring information security, the Secretary-General of the United Nations convened several Groups of Governmental Experts (hereinafter UN GGE, also the Group) in the field of information and communication in the context of international security[6]. UN GGEs have been tasked with proposing measures that could strengthen the security of global information and communication systems. Three out of five UN GGEs have prepared the corresponding recommendations[7].

4. The UN GGE reports reflect problems of international security regarding the use of ICT by states. The UN GGE has identified a number of problems in these international relations, to which the application and development of the norms, rules and principles of responsible behavior of states can be of significant importance. The UN GGE reports identify existing and potential threats to international peace and security, to which the norms, rules and principles of responsible behavior of states can be applied in order to create an open, safe, stable, accessible and peaceful ICT environment, as well as recommendations on areas cooperation of states in this field.

5. The most detailed recommendations for norms, rules and principles for responsibe state behaviour in the ICT environment are formulated in the 2015 UN GGE report[8]. These voluntary and non-binding norms, rules and principles UNGA has asked UN member States to «actively consider their recommendations and assess how they might be taken up for further development and implementation»[9].

6. An attempt to further develop the recommendations contained in the 2015 UN GGE report by the next UN GGE in 2016–2017, did not lead to the expected results. The experts could not agree on the issue of the application of international law to the use of ICT by states and were not able to prepare a consensus report on the results of their work[10]. According to the resolutions of the 73rd session of UNGA the study of implementation and development of norms, rules and principles of responsible behaviour in State use of ICTs continues in 2019–2021[11]. In 2019–2021 two expert groups will meet: the Open-ended Working Group (OEWG) open to all

5 Okinawa Charter of the Global Information Society. July 22, 2000. Okinawa (Japan)
6 2003-2004, 2009-2010, 2012-2013, 2014-2015, 2016-2017.
7 The 2010, 2013 and 2015 reports of the UN Groups of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201, A/68/98, A/70/174).*
8 Summary of the 2015 UN GGE report (A/70/174).
9 Summary of the 2015 UN GGE report (A/70/174).
10 Крутских А.В., Стрельцов А.А., International information security: problems and ways of resolving them. Forthcoming in Tikk, E. and Kerttunen, M. (editors) Routledge Handbook of International Cybersecurity. Routledge, 2020.
*11 A/C.1/73.1/L.27**

UN member states and and the UN GGE on the basis of equitable geographical distribution[12].

7. The 2013 and 2015 reports of the UN GGE note that "international law, and in particular the Charter of the United Nations, is applicable to international relations in the ICT environment and is essential for the maintenance of peace and stability, for the creation of an open, secure, peaceful and accessible information environment"[13]. In addition, "the importance of international law, the UN Charter and the principle of sovereignty as the basis for increasing security in the use of ICT by states" has been noted[14]. This view has been later recognized by UNGA that has endorsed 2013 and 2015 GGE reports, and by G7, G20, NATO, EU, SOC and BRICS in their statements and communiques[15].

8. As follows from the many materials of numerous conferences and seminars on ensuring international information security (cybersecurity), the international expert community has little common understanding of how international law should be applied to counter threats to international security and national security of states in the ICT environment[16]. There is also no agreement of the expert community on the issue of sources of international law in the field of counteracting threats to international peace and security arising from the trend in the development and use of ICT for military-political purposes. There are significant differences in the views of experts and on the role of the UN GGE in the progressive development of the relevant fields of international law.

9. The UN GGE 2015 report has not specified the relationship between its particular recommendations and international law[17]. It is therefore crucial to develop transparent and constructive approaches to maximize the stabilizing and peace-and-security-enhancing impact of norms, rules and principles that have been designed to promote an open, secure, stable, accessible and peaceful ICT environment.

10. In connection with the above, as well as increasing the intensity of ICT development as a factor in the development of the global information society, effective work in 2019–2021 of the UN GGE and the OEWG is of particular importance. In accordance with the mandates of the groups, they are entrusted with identifying the need for further development of the norms, principles and rules of responsible behavior of states in the ICT environment and in this context identify areas of development or adaptation of international law.

11. Many states and experts view the global ICT environment as a new space for international relations and, accordingly, the application of international law[18]. This circumstance gives rise to significant differences[19] in the interpretation of international law. The relative novelty of the issues of ICT security causes problems of ensuring legal certainty on disputed circumstances and reduces the predictability of State behaviour in these situations.

12. Differences in methodological approaches to the interpretation of the rules and standards of international law governing international relations in ICT environment are obvious in both scholarly work and national positions. Previous studies of the implementation of norms, rules and principles of re-

12 A/C.1/73.1/L 37

13 A/68/98, para 19, also para 24 of the 2015 Report.

14 A/70/174

15 See Qingdao Declaration of the Council of Heads of State of the SCO of June 18, 2018, Johannesburg Declaration of the Tenth Summit of the BRICS. July 26, 2018.

16 Tikk, E. And Kerttunen, M. Cyber treaty is coming. Чтоделать? Cyber policy institute, 2018.

17 For a more detailed discussion, see Крутских А.В.: The world is imposed with the concept of military measures in the digital sphere. http://russkoepole.de/ru/news-18/3913-v-krutskikh-miru-navyazyvaetsya-kontseptsiya-voennykh-mer-v-tsifrovoj-sfere.html; Tikk&Kerttunen, Parabasis: International cyber-diplomacy in stalemate. Norwegian Institute of International Affairs, 2018.

18 Russia and information security. International Conference. Moscow, December 20, 2016 г. Международная жизнь. Special Issue of 2017.

19 КрутскихА.В., СтрельцовА.А.. International law and the problem of ensuring international information security. Международнаяжизнь. 2014, 11; Стрельцов А.А. Adaptation of international law to the information space. Digital report, 2016; "Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary." Editor-in-Chief E. Tikk. Civil Society and Disarmament. Voluntary, UN. NY. 2017; State, business, civil society. Information Security. Materials of the 11th International Forum "Partnership of the State, Business and Civil Society at ensuring international information security. Supplement to the journal International Affairs. Garmisch-Partenkirchen, Germany, April 24-27, 2017

sponsible behaviour of States, designed to promote an open, secure, stable, accessible and peaceful ICT environment, indicates different positions to the issue[20]. Methodological differences have also been highlighted in the context of the *Tallinn Manual of International Law Applicable to Cyber Operations*[21]. This Manual has been promoted by some politicians and experts as the main source of knowledge about how to apply international law to issues of international cybersecurity[22]. Political contradictions became visible between states during the discussion of the problems of international information security and cybersecurity during the work of the UN GGE 2016–2017. Part of the problem is the lack of understanding among experts of the nature of the problems related to applying international law to international relations in the ICT environment.

13. The norms, rules and principles of responsible behavior of states in the ICT environment were welcomed by the UN General Assembly[23], but de facto have not been yet applied by states and, from this point of view, have yet to have regulatory impact on international relations. It can be assumed that over time and through state practice, norms, rules and principles of responsible behavior of states are likely to become a full-fledged component of "soft" international law. Although, the adoption of soft law does not create direct legal obligations for states and, accordingly, their non-compliance does not give rise to international legal responsibility of states, it nevertheless creates an opportunity to draw the attention of the international community, through the use of the information sphere, to the behavior of states in the ICT environment. As noted by the UN GGE (2015), the proposed standards will reflect "the expectations of the international community" and define "standards of responsible behavior", the application of which "will allow the international community to assess the actions and intentions of states."[24] It can be expected that gradually these norms, rules and principles of responsible behavior of states will acquire de facto status as international law, possibly customary international law.

14. Currently, the study of problems of legal regulation of international relations in the implementation of norms, rules and principles of responsible state behaviour in the ICT environment remains of a theoretical nature and is based on hypothetical scenarios.

15. This study is aimed at identifying ways to better understand the problems in the legal regulation of international relations in the ICT environment and discussing possible ways to develop the norms, rules and principles of responsible behavior of states in the ICT environment, as well as ways to develop international law that creates the conditions for legal regulation of relationship. The study will identify the problems of applying international law to the ICT environment and to facilitate the search for their practical solutions.

16. To achieve the objectives of the study, it is important to formulate a common approach to assessing the applicability of the norms, rules and principles of responsible behavior of states in the ICT environment to regulate relevant international relations. It is assumed that the applicability of these norms, rules and principles is characterized by the following: a) the possibility to implement these norms, rules and principles on the basis of the principles and norms of international law by the States, including the practice of states in using the means of peaceful resolution of international disputes arising from incidents in the ICT environment ; b) the possibility to implement these norms, rules and principles by authorized international organizations and institutions to contribute to the resolution of

20 Streltsov A.A. Recommendations regarding the rules and principles of responsible behavior of states to ensure an open, safe and peaceful ICT environment. Digital report. 28.04.2016; Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology A Commentary. Editor-in-Chief E. Tikk. Civil Society and Disarmament. Voluntary, UN. NY. 2017; State, business, civil society. Information Security. Materials of the 11th International Forum "Partnership of the State, Business and Civil Society at. Ensuring international information security. Supplement to the journal International Affairs. Garmisch-Partenkirchen, Germany, April 24-27, 2017

21 Michael N. Schmitt, Tallinn Manual of International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2013).

22 A/72/327

23 A/73/505, 19.11.2018

24 A/70/174

international disputes arising from incidents in the ICT environment.

17. It can be assumed that common understandings of the positions of national states and the positions of the international expert community on the application of voluntary and optional norms of responsible behavior of states will contribute to the successful search for means to counter threats to international peace and security, the prevention of crises and conflicts caused by incidents in the ICT environment, and will contribute to the use of ICTs and the development of the global economy and national societies. Greater agreement could also help prevent relevant misperceptions and misunderstandings in assessing situations related to the use of ICT by states, thus ensuring national or international security. This study creates the basis for a discussion of the methodology for the study and application of voluntary, optional norms, rules and principles of responsible behavior of states in the ICT environment[25].

18. While the principal focus of this study relates to state behavior and the legal implications of state action in cyberspace, the operational reality of securing cyberspace requires the cooperation of a multitude of non-governmental stakeholders, including private companies, technical experts, and, as in this study, academic and civil society organizations. Such so-called multi-stakeholder or multi-party approaches are in themselves not universally agreed in that some perceive them to conflict with state sovereignty or states' principal responsibility for ensuring national and international security. At the same time, no state can secure its own cyberspace without the cooperation of multiple parties who own and service the core infrastructure of the Internet. Any successful implementation of international law in cyberspace will require the participation of such parties, and, as such, they must be consulted as to the practicability and effectiveness of proposed norms, policies, and agreements that they will be required to implement. Many useful processes already exist that create such consultations and contribute constructively to the evolution of mutual understanding and acceptance of what constitutes responsible behavior[26].

19. In order to further study the problems of applying international law in the OEWG, it is advisable to actively involve specialists of international law related to the use of ICTs to ensure national and international information security (cybersecurity), as well as expertise on the functioning of the ICT environment.

III. METHODOLOGICAL REMARKS

20. As noted earlier, experts differ significantly in assessing the legal content of voluntary, non-binding norms, rules and principles of responsible state behavior in the ICT environment, as well as in assessing the possibility of applying international law to the behavior of states in the ICT environment. With this in mind, it is essential to clearly define the structure and the process of this study, to allow comparing the positions of experts on the issues under discussion, to clarify the causes and content of differences in the interpretation of recommendations.

21. In the present study, each analyzed recommendation is considered first contextually and then substantively. This contextual analysis identifies the field of international relations that has a significant impact on international security; the area of international relations to which the regulatory impact of the recommendation is directed; and the purpose of the recommendation in question, i.e. the result to be achieved as a result of the application of the recommendation. Accordingly, the discussion of each

25 Materials of the work of the Group of Governmental Experts on achievements in the field of information and telecommunications in the context of international security 2016-2017.

26 Examples include the Global Commission on the Stability of Cyberspace (for which the EastWest Institute served as Secretariat) www.cyberstability.org, as well as Global Forum on Cyber Expertise (GFCE), World Summit on the Information Society (WSIS), the Global Commission on Internet Governance, the Internet Governance Forum (IGF), the Global Conference on CyberSpace (GCCS), the NETmundial Initiative, the Organization for Security and Co-operation in Europe (OSCE), the African Union Commission (AUC), the Charter of Trust, the Cybersecurity Tech Accord, the United Nations Institute for Disarmament Research (UNIDIR), the Paris Call for Trust and Security in Cyberspace, and the UN Secretary-General's High-level Panel on Digital Cooperation. The ICT4Peace Cybersecurity Policy and Diplomacy Capacity Building Program.

norm follows a systematic inquiry asking questions about the *subject*, *object* and *purpose* of the norm, followed by selected challenges of implementation.

22. The study creates a basis for initiating discussion of the content of the identified problems by interested specialists.

23. For each recommendation, authors of the study have offered views as to specific issues related to the implementation. This part of the analysis is to draw attention to practical considerations that those planning to implement the proposed recommendations, might want to additionally discuss or clarify.

PART II

IV. GENERAL PROBLEMS OF APPLYING INTERNATIONAL LAW TO THE ICT ENVIRONMENT

IV.1. The role of states in the implementation of the norms, rules and principles of responsible State behaviour

24. According to paragraph 28 b) of the 2015 UN GGE report, "in their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States." Furthermore, State sovereignty, international norms and principles arising from the principle of State sovereignty apply to the behaviour of States in activities related to the use of ICT[27], as well as to the jurisdiction of States over the ICT infrastructure in their territory[28].

25. This chapter is devoted to the consideration of the sovereignty of states in the ICT environment as a prerequisite for the emergence of the practice of interpreting the content of norms and principles of international law to the application of ICT by states, as well as the implementation of these norms and principles. The authors proceed from the assumption that despite numerous differences in political interpretation and practical application of sovereignty by states in modern geopolitical reality[29], and particularly in the context of the use and development of ICTs, this notion remains a fundamental common denominator to guide the discussion on the applicability of international law to the ICT environment[30].

26. State sovereignty refers to the supremacy, finality and independence of State authority both in the State's territory and in relations with other countries. In foreign relations, the sovereignty of the State is manifested in the complex of rights and powers of the state determined by the principles and rules of international law, enshrined in international treaties adopted by states, as well as in international customs reflecting universal practice. Sovereignty is also expressed in general principles of law recognized by civilized nations. In foreign relations the sovereignty of the State is also manifested in the exercise of sovereignty whereby States do or do not take international obligations upon them.

27. A State's territory is formed by a set of physical environments within which States exercise sovereignty, i.e. their legal authority and jurisdiction. A State's territory includes land with its subsoil, water territory (internal waters and territorial sea of the state), as well as airspace. The territory of a State has borders recognized by other States. Recognition of State borders is achieved through the conclusion of relevant treaties with neighbouring States, as well as official statements on this issue by authorized bodies of other States.

28. The object of sovereignty, in the context of this study is the ICT environment. According to the 2015 UN GGE report, the goal of the UN GGE work is to achieve an ICT environment characterized by openness, security, stability, accessibility and peacefulness[31].

---

27 Information technologies are processes, methods of searching, collecting, storing, processing, providing, disseminating information, as well as ways to implement such processes and methods. Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection". ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning. ICTs are often spoken of in a particular context, such as ICTs in education, health care, or libraries. The term is somewhat more common outside of the United States. www.earchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies

28 A/68/98, para 20.

29 For example, see (1) https://www.comparativepolitics.org/jour/article/viewFile/123/139; and (2) https://www.japantimes.co.jp/opinion/2015/09/21/commentary/world-commentary/nature-sovereignty-key-issue-russia-u-s-divide/.

30 State sovereignty is the property of the state, independently and independently of the authority of other states, to exercise its functions on its territory and beyond, in international communication. In Козлова Е.И., Кутафин О.Е.. Конституционное право. М., Юристъ. 2004, стр.165;«Perhaps the outstanding characteristic of a state is its independence, or sovereignty. This was defined in the Draft Declaration on the Rights and Duties of States prepared in 1949 by the International Law Commission as the capacity of a state to provide for its own well-being and development free from the domination of other states, providing it does not impair or violate their legitimate rights.» Malcolm N. Shaw. International law. Cambridge. University press. N.Y., 2008. p. 211.

31 p. 2, A/70/174.

29. Reaching an international consensus on practical application of state sovereignty in the ICT environment would require a shared understanding of the nature of existing disagreements between states on this matter with a clear distinction between political and technical differences about the exercise of sovereignty and jurisdiction delimitation in the sphere of ICTs.

Remark. Opinions diverged regarding the content of political differences in the study group. According to some participants in the study, the contradictions are caused, first of all, by the focus of some states on such issues as applying jurisdiction to key parts of the Internet government system, "hostile" and "malicious" use of ICTs to resolve interstate contradictions, the use of private parties for this, as well as abusing of freedom for distribution of unreliable information. According to other participants in the study, contradictions arise due to the focus of some states on excessive state regulation of relations in the field of restrictions on freedom of information.

IV.2. The definition of ICT environment

30. In Russian political doctrine, an analogue of the ICT environment is the concept of "information sphere", which is described as "a set of information, objects of informatization, information systems, sites in the information and telecommunication network" Internet "(hereinafter - the Internet), communication networks, information technologies, entities whose activities are associated with the formation and processing of information, the development and use of these technologies, ensuring information security, as well as a set of regulatory mechanisms corresponding social relations[32].

31. In the political doctrine of the United States, a close analogue of the ICT environment is also the concept of "information environment", which is seen as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information[33].

32. From the point of view of the physical nature of the processes taking place in the ICT environment, this environment can be considered as "cyberspace" — by a doctrinal US definition "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[34].

33. An important component of the ICT environment is the information infrastructure, which provides the possibility of automated processing of information (in particular, its production or storage) and communication (receipt, transmission and dissemination) of data in various spheres of society[35].

IV.3. Distinct features of the ICT environment

34. Important features of the ICT environment that distinguish it from the traditional spaces of maintaining friendly and peaceful international relations are: the global ICT environment, due to the dependence of its functioning on the participation of interested citizens, organizations located in different jurisdictions[36], as well as states (the vast number of direct and indirect actors and stakeholders); the artificial nature of the ICT environment, due to the integration of computing and communication

32 The Doctrine of Information Security of the Russian Federation. The Decree of the President of the Russian Federation of December 5 2016 г. № 646
33 US Department of Defense, DOD Dictionary of Military and Associated Terms (JP 1-02) (June 2019), and Strategy for Operations in the Information Environment, (June 2016).The latter explains (p. 3) the notion of Information Environment asa heterogeneous global environment where humans and automated systems observe, orient, decide, and act on data, information, and knowledge. With its function as a conduit for influence on decision-making and command and control, the IE is a key component of the commander's operational environment. Characterized by ubiquitous on-demand media and interpersonal hyper-connectivity, today's IE enables collaboration and information sharing on an unprecedented scale."
34 US Department of Defense, DOD Dictionary of Military and Associated Terms (JP 1-02) (June 2019).
35 Information infrastructure - a system of organizational structures, subsystems that ensure the functioning and development of the country's information space and means of information interaction. It includes: a set of information centers, subsystems, data and knowledge banks, communication systems, control centers, hardware and software tools and technologies for collecting, storing, processing and transmitting information. Provides consumer access to information resources. https://kartaslov.ru/
36 For further discussion of this broader communities, see paragraph [#18#] above.

devices, systems and networks in its composition, using the global system of digital identifiers; multi-level system of open protocols for the interaction of devices and systems, which are realized on the computers, communication and other devices. These technologies are a combination of methods and algorithms for processing information in computing and communication devices, systems, networks.

35. An important consequence of the artificiality, digitaland distributed nature of the ICT environmentare difficulties to observe and objectively register the processes of ICT use, through which access to public and private systems and possibility of targeted dissemination of information are provided, which allows states to influence and exercise control over the processes of socio-political development of society, and ensure deniability of unlawful interference in the internal affairs of sovereign states[37]. Such interference may threaten national security and regional and international peace, security and stability.

36. Difficulties in monitoring the use of ICTs by states create significant difficulties detecting and establishing causal relationships between actions of states and their consequences as well as assessing the real and expected consequences of such actions. This can explain the lack of detailed substantiation that has become a frequent practice: attribution of responsibility by affected states[38] to states allegedly sponsoring cyber attacks; the existence of an objective connection between the incident in the ICT environment and the state to which responsibility for the incident is attributed.

37. The fact that the processes in the ICT environment are virtual (i.e. may easily be presented as real processes, personalities and events while in fact being imaginary) and, together with the limited capabilities of the national authorized bodies for an objective, legally reliable analysis and even detection of incidents in the ICT environment, makes technically and legally sufficient attribution a very difficult task. Difficulties in objective, legally reliable recording of incidents in the ICT environment can lead to politicized assumptions about the possible parties to these incidents and the motives for corresponding actions[39]. This creates significant problems in the application by states of international law to international relations in the ICT environment.

38. The lack of observability of the processes by which states use ICTs also complicates the assessment of alleged damage from dangerous actions in this area and complicates the legal assessment of the actions of states in the field of ICTs, which create the preconditions for threats to international peace and security.

39. Consequently, one can conclude that the ICT environment as an object of international law is a legal fiction. This fiction consists in attributing to the ICT environment the properties of the traditional territory of the state and extending state sovereignty to it.

40. Insufficient understanding on how to apply international law to relations in the ICT environment determines the relevance of the discussion of the following problems: (a) determination of the content of international obligations of states in the ICT environment; (b) legal consolidation of the spatial limits of the sovereignty of states in the ICT environment; (c) definition of issues that fall within national regulatory competence.

IV.4. Desired characteristics of the ICT environment

41. The three groups of UN government experts working in 2009–2010, 2012-2013 and 2014–2015 have emphasized that the ICT environment should be open, secure, stable, accessible and peaceful. Achieving these qualities should be achieved, among other things, as a result of the application by states, international organizations and institutions of the norms, rules and principles of responsible behavior. To assess the current state of "openness", "security", "stability", "accessibility" and "peacefulness"

37 On soft law in this field, see for example, UNGA, "Respect for the principles of national sovereignty and non-interference in the internal affairs of States in their electoral processes", A/44/147 (15 December, 1989).

38 "State is a victim" - a state that claims to cause him substantial damage as a result of a "cyber attack" on objects of its information infrastructure.

39 Kazakovtsev, A.V., NATO and Cybersecurity. News. Volgograd State University. Ser. 4, History. 2012, №2 (22).

of the ICT environment, it is important to determine the content of these qualities.

42. As these terms can be understood differently, the following constitutes one possible way of explaining them.

43. Openness of the ICT environment lies in the possibility of its use by people living in all countries of the world, through access of people to global information resourses and the integration of national ICT environments into the global ICT environment.

44. Security refers to the ability of States, organizations and individuals who design, develop and use information infrastructure and related services to counter threats to the human rights, individual, organizational and other components of the national security, the functionality of the systems and services as well as to international security and peace.

45. Stability lies in the ability of the information infrastructure to ensure the fulfilment of the tasks of the development and functioning of the information infrastructure, as well as the maintenance of the national and global information sphere in the event of disruption of the operation of individual infrastructure elements.

46. Accessibility refers to the constant readiness of the information infrastructure to meet legitimate needs, to realize the rights and fulfil the duties of the subjects of the society (human, commercial and non-commercial organizations, public authorities), to provide automation services for processing and communication of information as well as access to information.

47. Peacefulness is ability of the information infrastructure to contribute to the stable development of society, the peaceful resolution of international disputes in such a way that international peace and security and justice[40] are not endangered, to not allow the threat or use of force against the territorial integrity or political independence of any State, or in any other way incompatible with the purposes of the United Nations[41].

40 UN Charter, Article 2(3).
41 Ibid., Article 2(4)

PART III

V. IMPLEMENTATION OF NORMS, RULES AND PRINCIPLES OF RESPONSIBLE BEHAVIOUR OF STATES

48. This section presents the results of discussions between the project participants on the practical application of the recommendations in paragraphs (g), (h) and (k) of paragraph 13 of the Report of the Group of Governmental Experts in the Field of Informatization and Telecommunications in the Context of UN International Security (2015).

49. During the discussion, the rules and principles of international law were considered, which the project participants concluded to be applicable to the recommendations in question.

50. The rules and principles of international law referred to by the project participants in the discussion do not exhaust the many other sources of international law that could be applied to the regulation of the considered groups of international relations.

51. The results of the discussions illustrate the possible political and legal consequences of the unresolved issues addressed in Section II on the implementation of international relations on the basis of international law.

52. When considering the conclusions and recommendations formulated by the project participants, the following should be considered: (a) existing international law was created to regulate the relations between sovereign, equal states; (b) interstate relations in the ICT environment are partially formed regarding the objects of the intangible space (information, ICT, information and communication activities) and partially regarding tangible objects (devices, systems, and physical communication networks), as well as human behavior in this sphere, space and environment, which some experts regarded differing significantly from the point of view of using legal means from the material space.

53. It is hoped that the conclusions and recommendations proposed by the project participants can contribute to and further inform the discussion on the application and development of international law.

V. 1. Paragraph 13 (g) of the UN GGE 2015 Report

The subject, object and purpose[42] of the recommendation

54. According to paragraph 13 (g) of the 2015 Report, States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

55. The UN General Assembly has noted the need to strengthen the links between the most important infrastructures of countries (often referred to as critical infrastructure (CI)), and the information infrastructure as the latter increasingly ensures and influences the interconnectivity and functioning of critical infrastructure[43].

56. The UN GGE has noted the existence of alarming trends in the global ICT environment, including the dramatic increase in the number of cases of malicious use of ICT by state and non-state actors that "pose a threat to all states" and can "damage international peace and security"[44]. According to the experts, “a number of States are developing ICT capabilities for military purposes” and “the use of ICTs in future conflicts between States is becoming more likely”[45]. “The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical

42 The subject of recommendations is the field of interstate relations, which is essential for creating an open, secure, stable, accessible and peaceful ICT environment. The object of the recommendations is a group of interstate relations, the regulation of which is directed to the legal impact of optional, voluntary norms, rules and principles of responsible behavior of states; The purpose of the recommendations is to create legal conditions that ensure the desired behavior of states in relations consisting of the object of recommendations.

43 Creating a global culture of cyber security and protecting critical information infrastructures. Resolution of the UN General Assembly, A/RES/58/199.

44 A/70/174

45 A/70/174

infrastructure is both real and serious"[46]. "The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security". "The diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk. States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy"[47].

57. The proposed recommendation calls for voluntary exercise of the authority of States to ensure the protection of the CI as well as information infrastructure that is the technical basis for the operation of the critical infrastructure.

58. The subject of regulation in this recommendation is the functioning, sustainability and safety of the information infrastructure. As all information infrastructure is subject to territorial jurisdiction, the implementation of this recommendation requires States to a) identify infrastructure important or critical for them, and b) resolve its functioning, sustainability and safety within their jurisdiction. It is assumed, that by providing adequate protections to national critical infrastructure and the national segment of critical information infrastructure, States reduce threats to international peace and security.

Remark. The Russian concept of international information security refers to a triad of such threats as threats of criminal, terrorist and military-political nature. The American approach to international cyber security emphasizes the countering the threats of the military use of ICTs, with substantial attention to criminal and terrorist threats as a matter of law enforcement and homeland security in cyberspace[48].

59. The object of this recommendation is international relations in the field of international security related to the functioning, sustainability and safety of national critical infrastructure.

60. The purpose of recommendation is to create conditions for each State to achieve a sufficient degree of national security by assuring that the functioning of the critical infrastructure is adequately protected against "existing and emerging threats from uses of ICTs, by States and non-State actors alike, that may jeopardize international peace and security"[49]. This recommendation aims at a situation, where information infrastructure and critical infrastructure of other States are also adequately protected from the outlined threats. It is expected that by implementing this recommendation, States will be able to draw attention of the international community to the consequences arising in the case of a violation of the functioning, sustainability or safety of relevant infrastructure due to the inadequate level of security, including the compensation of damages resulting from such circumstances.

61. The measures taken to protect critical infrastructure and information infrastructure under a State's jurisdiction should consider the threats outlined by the GGE, in particular in paragraphs 4 to 7 of the 2015 report.

Further considerations for implementing the recommendation

62. As States are to provide the safety of their critical infrastructure as well as information infrastructure under their jurisdiction, this recommendation can be implemented in international and national law, policy and strategy. Implementation can be directed at creating the conditions for cooperation between interested national and international stakeholders.

63. In international law, several mechanisms have been developed that can be applicable to the

46 A/70/174
47 A/70/174
48 International Strategy for Cyberspace, 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; Department of State International Cyberspace Policy Strategy, 2016, https://www.hsdl.org/?view&did=792759
49 Foreword by the Secretary-General. A/70/174

protection of critical areas, objects, functions and services[50].

64. Appropriate measures to protect information infrastructures may include, *inter alia*, activities to identify threats and reduce the vulnerability of critical information infrastructures, minimize damage and recovery time in case of damage or attempts to breach protection, and identify the causes of damage or the source of such attempts, the effectiveness of which may be increased, for example, by exchanging information on best practices among States as well as offering advice and assistance or other forms of cooperation.

65. International cooperation of States related to the application of the commented recommendation can comprise facilitating the development of national risk reduction strategies for protecting critical infrastructure and information infrastructure under national jurisdiction, considering the following elements of protection[51]:

a) making available communication networks for urgent warning of vulnerability, threats and incidents in cyberspace;

b) increasing the level of awareness among interested States about the nature and extent of their critical infrastructure and information infrastructure under their jurisdiction, as well as the role that States play in protecting these infrastructures;

c) analysis of the structure of the relevant infrastructures and identification of factors that determine their interdependence and are important for strengthening the protection of such infrastructures;

d) promoting the development of partnerships between stakeholders representing both the public and private sectors to exchange information about the most important infrastructures and its analysis in order to prevent damage to such infrastructures or attempts to violate their protection, as well as to investigate cases of damage to the objects of protected infrastructure;

e) creating and maintaining of communication systems in a crisis situation and verification of their functioning to ensure reliable and stable information interaction in emergency situations;

f) Ensure that data availability policies take into account the need to protect critical information infrastructures.

g) facilitating the monitoring of attempts to break into the protection of the protected infrastructure facilities and, as appropriate, providing information on the results of such tracking to other states;

h) organizing professional preparedness and training to strengthen the response capacity, testing of continuous work plans and reserve plans in the event of attempts to crack the protection of the critical infrastructure facilities, and encouraging stakeholders to participate in similar activities;

i) making available adequate material and procedural legal regulation, as well as qualified personnel to investigate attempts to violate the protection of critical infrastructure and information infrastructure facilities, identify and bring to justice those involved in these attempts, as well as the established procedure for coordinating such investigations with other states;

j) participating in international cooperation in the field of ensuring the protection of protected facilities, including by establishing and coordinating the work of communication networks for urgent warning systems, exchanging information on vulnerabilities, threats and incidents, and analysing such information, as well as coordinating investigations into attempts to break security of such infrastructures in accordance with national legislation;

k) promoting national and international research and development and promote the use of protection technologies that meet international standards.

66. An important direction of the international cooperation in this field could be the participation

50 For example, the Convention (No.174) concerning the Prevention of Major Industrial Accidents (Geneva 1993)Convention on the Physical Protection of Nuclear Material (Vienna 1979); Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal 1971); Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Rome 1988).

51 Resolution of the UN General Assembly "Creating a global culture of cyber security and protecting critical information infrastructures" of December 23, 2003, A/58/199.Annex Elements for protecting critical information infrastructures

of states in the improvement of the system of international standards for technical regulation[52] to ensure an appropriate level of technical protection and organization of management of the information infrastructure facilities that support the operation of the critical infrastructure.

67. To enhance trust and cooperation and reduce the risk of conflict, the UN GGE recommends that States consider the following voluntary confidence-building measures[53]

(a) The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;

(b) The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents;

(c) Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;

(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:

i. A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;

ii. The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;

iii. The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;

iv. The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents[54].

Problems of implementation

68. Under specialized regimes of international law, cooperation on critical infrastructure protection is also coordinated via sectorial entities like IAEA, IMO or ICAO. While international agreements exist that apply standards and requirements of protection to certain objects, sectors, functions and services, these do not cover all critical infrastructure.

69. At the same time, there is no universal framework for cooperation and coordination on creation of a global culture of cybersecurity. The respective resolution[55] contains guidance to be considered at national level without addressing particular international frameworks or platforms of cooperation.

70. Inadequate protection of critical infrastructure or national information infrastructure may lead

52 ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cyber security; ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems – Requirements; ISO 22301 Societal security -- Business continuity management systems --- Requirements; ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security; ISO/IEC 27035 Information technology -- Security techniques -- Information security incident management; ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management; FIPS 140-1: Security Requirements for Cryptographic Modules; FIPS 186-3: Digital Signature Standard.

53 A/70/174

54 UN A/70/174

55 Global Culture of Cybersecurity UN Resolution. 64/211 (2010).

to an international dispute. In case of a dispute involving the recommended actions, the following shortcomings in international law are likely to influence resolving international disputes:

a) absence of internationally agreed criteria of critical infrastructure;

b) absence of sufficient and commonly understood criteria of adequate safety of such infrastructure;

c) lack of evidence or confirmation of ICT incidents affecting critical infrastructure and national information infrastructure

d) lack of internationally agreed procedures for conducting relevant investigations.

71. In order to address the above gaps, voluntary efforts by States could be directed at (a) establishing or consolidating of the framework of national information infrastructure (for example, lists of objects included in this concept), as well as (b) determining the procedure for conducting joint investigations in case of incidents in the national ICT environment concerning its stability. Such recommendations could be part of universal, regional, multilateral peaceful systems to ensure the security of critical information infrastructure from threats in the field of ICT.

V. 2. Paragraph 13 (h) of the UN GGE 2015 report

Object, subject and purpose of regulation

72. According to paragraph 13 (h) of the report, States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

73. The implementation of this recommendation could be considered as a way to apply the principles of friendly relations and cooperation among states and a contribution to the achievement of the UN goals.

74. States have repeatedly stated the need for joint actions aimed at eliminating threats caused by the malicious use of ICT[56]. It is necessary to consider joint measures to strengthen international peace, stability and security. Such measures include the development of a common understanding with respect to the application of relevant norms of international law and the norms, rules and principles of responsible behaviour of states that follow from them. Further, States should intensify cooperation in combating the use of ICT for criminal or terrorist purposes, properly harmonize their legal approaches and develop practical cooperation between relevant law enforcement agencies and prosecutorial authorities[57].

75. Malicious activities in the ICT environment can cause serious damage to the economy as well as national and international security. They can be directed equally against physical and legal persons, national infrastructure and governments. They can be associated with a significant risk to public security, the security of countries and the stability of the international community as a whole, integrated into the global network.

76. Over the past decade, UN member states "have repeatedly reaffirmed the need for international cooperation in addressing threats to ICT security in order to combat the malicious use of information technology for criminal purposes, the creation of a global culture of cybersecurity and the promotion of other important measures that can reduce the risk to the stability of the functioning and security of the use of information infrastructure."[58]

77. The object of the recommendation is international relations in the field of mutual assistance.

78. The subject of the recommendation is the voluntary commitment of States to a) assist other States whose critical infrastructure has become the target of malicious acts (criminal, terrorist, hostile) in the field of ICT, and b) facilitate the mitigation of the consequences of malicious acts in the field of ICT directed against critical infrastructure.

*56 A/68/98**
57 A/65/201, para. 12
58 A/65/201

79. It is assumed that national infrastructure of the State requested to provide assistance has been used to commit malicious acts in question or that the requested State has relevant capacity to provide such assistance. It is further assumed that the malicious act in question has influenced the functioning of the critical infrastructure and that assistance would reduce the severity of the consequences of malicious acts against the requesting State.

80. The purpose of the recommendation is to create legal conditions for strengthening the sustainability of critical infrastructure functioning, sustainability and safety by reducing the negative impact of malicious actions in the field of ICT on critical infrastructure, and, thereby, enhance international peace and security.

Further considerations for implementing the recommendation

81. The commented norm addresses voluntary assistance to other States due to the emergence of the ICT environment as a new milieu of international relations.

82. International law potentially applicable to the issues in question follows, *inter alia*, from the provisions of the UN Charter, the Declaration of Principles of International Law[59], the Assistance Convention[60], the Convention on the Transboundary Effects of Industrial Accidents[61], the Convention on the Provision of Telecommunication Resources[62]. Some times the assistance can also be based on the United Nations Convention against Transnational Organized Crime[63].

83. In accordance with UNGA Resolution 57/150 of 16 December 2002, each State is primarily responsible for providing assistance to victims of natural disasters occurring on its territory, and therefore the affected State should play a major role "in initiating, organizing, coordinating and providing humanitarian assistance on its territory".

84. Currently, there is no specific binding international obligation of the States on assistance in emergencies arising from malicious acts in the field of ICT against the national segment of critical information infrastructure.

Remark. Some experts underscored the mechanisms of multilateral mutual assistance in criminal law and other legal matters as an international framework that is binding and can provide the basis for assistance.

85. There are currently no widely acknowledged examples of the application of "soft law" rules for the regulation of international relations in the field of providing assistance and mitigating the consequences of the malicious use of ICT against the national CII.

Remark. Some experts held a view to the contrary. There are many examples of successful cooperation and assistance between states in case of cyberattacks, for instance between first responders, law enforcement agencies as well as between diplomats and political decision-makers.

86. The main problem of the implementing the recommendation in question relates to the difficulty of identifying the State from whose territory the malicious acts against the national segment of critical information infrastructure or national critical infrastructure are occurring. This complicates applying legal procedures for resolving international disputes or misunderstandings.

Remark. Some experts held the view that it should be of interest of all, and especially those wrongfully attributed, to solve the issue cooperatively rather than denying their involvement or offering no comment. These experts concluded that

59 Resolution 2625 of the UN General Assembly on October 24, 1970

60 Convention on Assistance in the Event of a Nuclear or Radiological Emergency. General Conference of the International Atomic Energy Agency. September 26, 1986.

61 Convention on the Transboundary Effects of Industrial Accidents. Helsinki, 17 March 1992, E/ECE/1268.

62 The Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations. Tampere. June 18, 1998.

63 United Nations Convention against Transnational Organized Crime (Palermo 2000).

the main problems of the implementation relate to the potentially sensitive nature of the incident and the varying capabilities states have to meaningfully offer assistance without risks of compromising their own security."

V.3. Paragraph 13 (k) of the UN GGE 2015 Report

Object, subject and purpose of regulation

87. According to recommendation 13 (k), States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

88. The following principles apply to the implementation to this recommendation:

a) "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory"[64];

b) "No State or group of States has the right to interfere directly or indirectly for any reason in the internal and external affairs of any other State";

c) "No State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind.[65]"

89. The subject of the recommendation is the independence and unhindered performance of national computer security incident response teams (CSIRTs).

90. The object of this recommendation is relations between States in conjunction with prevention, detection, response to and recovery from ICT incidents. In such relations, authorized CSIRTs play an active and central role. It is assumed that CSIRTs exercise powers and responsibilities in the field of incident response related to national critical information infrastructure. Information systems[66] of CSIRTs support the implementation of the tasks assigned to them.

91. The purpose of this recommendation is creating conditions for the voluntary acceptance by States of international obligations related to the prohibition of activities in the field of ICT, which could damage the information systems of CSIRTs and the established trust on them. This recommendation aims at preventing the use of authorized CSIRTs to carry out malicious international activities. It also seeks to ban conducting and knowingly supporting actions of State-run structures that aim, or conclude, at inflicting damage on the information systems of CSIRTs as one of the elements providing the security of the national segment of critical information infrastructure.

Further considerations for implementing the recommendation

92. Prohibiting deliberate activity, or support to, inflicting damage on CSIRTs essentially means granting these entities special international guarantees of security. This can be achieved by establishing a special political or legal international regime for CSIRTs.

Currently, the violation of the prohibition in this recommendation can be interpreted as a violation of the principle of non-intervention in domestic affairs, as provided by international law. According to this binding principle, States are obliged not to in-

64 A/68/98.

65 Declaration on the principles of international law concerning friendly relations and cooperation between states in accordance with the UN Charter. Resolution 2625 of the UN General Assembly on October 24, 1970.

66 In the Russian Federal Law "On Information, Information Technologies and Information Protection" (No. 149-FZ), the notion of "information system" is disclosed as "the aggregate of information contained in databases and providing information technology and technical means for processing it." US Law uses the term "information system" as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" (44 USCS § 3502, https://definitions.uslegal.com/i/information-system/); Encyclopedia Britannicauses the term "Information system" as "an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products", (/www.britannica.com/topic/information-system).

terfere in matters falling within the internal jurisdiction of any other state. Such jurisdiction comprises the legally established regime of security of national CSIRT information systems.

93. The voluntary observance of the proposed prohibition is one of the means of ensuring an open, secure, stable, accessible and peaceful. The prohibition of the use of the CSIRTs for malicious international activities can be achieved through formulating relevant international obligations as well as application of regulatory legal acts of national legislation.

94. At the same time, incidents may referred to events that interrupt the procedure for processing information recorded, which have significant negative consequences for the quality of the functioning of national facilities. In particular, such incidents may include the consequences of malicious software, denial-of-service attacks, unauthorized access to information and other unlawful actions.

95. Authorized CSIRTs can be both governmental and non-governmental organizations operating on a commercial basis. Their competence is established by national legislation. A CSIRT may respond to incident by:

a) confirmation or refutation of the very fact of the incident;

b) collecting reliable information about the incident; control over the correctness of the detection and collection of facts; protection of civil rights established by law and security policy;

c) minimizing the impact on business and network operations; the formation of civil and criminal lawsuits against violators;

d) creating an accurate report and useful recommendations for future reactions to incidents, etc.

96. Violation of this restriction could include examples, where a State that has accepted the obligation to comply with prohibition, engages in malicious use of ICTs against other states and the information systems of their authorized CSIRT; or where a State that has not accepted the obligation to comply with the prohibition of using the CSIRT, carries out malicious acts against national critical information infrastructure of other states.

97. There are currently no examples of the application by States of "soft law" norms for the regulation of international relations in the field of ensuring the protection of the information systems of the CSIRTs.

Remark. This view was not supported by some experts, who noted that the wide and trusted cooperation between CSIRTs offers guarantees not just continued cooperation in case of an incident or even crisis but also of CSIRT inviolability. Moreover, they referred to the UN Charter as such and the prohibition of the use of force and of interventions as already offering both legal protection and globally accepted guidance on state behaviour applicable in the ICT environment or cyberspace.

99. The application of this recommendation is complicated due to the lack of the possibility of using legal measures for resolving relevant international disputes or misunderstandings. In particular, the Russian authors consider the following practices problematic:accusations against States for the malicious use of ICTs against the information systems of the national segment of information infrastructure, as well as for the malicious use of CSIRTs for harming the national segment of information infrastructure; attribution of responsibility to States for the conduct of, or deliberate support to, activities designed to harm the information systems of SCIRTs;accusing States of carrying out malicious international activities[67]. In modern conditions such charges, as a rule, don't have any legal basis, what is rising the risk of attribution for responsibility to States on the political point of view only.

Remark. Other experts underscored that the option of applying the law of peaceful settlement of international disputes is always open to states. This problem is particular to strategic contestants but does not necessarily reflect the views and experience of all states. They agreed that attribution remains problematic, but largely to insufficient national capacities.

67 Крутских А.В., Стрельцов А.А.. Международное право и проблема обеспечения международной информационной

99. The above issues contribute to the risk of an international dispute that may not have the prospect of being resolved through legal means.

100. For some participants, measures to achieve the purpose of the recommendation included: a) reaching an agreement on the establishment of an international organization authorized to conduct investigations of international incidents in the ICT environment, involving CSIRTs;b) developing recommendations for conducting such investigations with the participation of representatives of interested states; c) adoption of recommendations on the list and characteristics of malicious international activities.These proposals do not reject further dialogue on all range of the possible directions for cooperative expert study of all other offers.

Remark. Other experts recommended further dialogue on how to implement this particular recommendation and an exchange of national views on the matter. They were also skeptical of the need and meaningfulness of an international investigation or attribution organization.

VI. Conclusions and recommendations

101. States can, and must, apply international law to international relations in the ICT environment. Current uses of ICTs by States can generate international disputes and lead to a threat or breach of international peace and security. To improve the effectiveness of the application of international law to relations in the ICT environment, UNGA has asked states to explore possible directions for the progressive development of international law.

102. At this stage of international relations, the adoption of norms, rules and principles of responsible behaviour of States in the ICT environment is a more promising prospect than any specific study of international law or binding commitments by States.

103. The mechanism of voluntary and non-binding norms, rules and principles, is intended to help to the producing of more refined international norms by way of constant and uniform State practice. The process of discussing norms of responsible State behaviour in the use of ICTs can also inform States of their mutual expectations, best practices and experience.

104. The current stage in international relations allows the academic community and policy-makers study the possibility of practical implementation of the proposed norms, rules and principles of responsible behaviour of states. To achieve strong and universal standards of behaviour, "soft law", i.e. the norms of which are not legally binding and whose breaches do not entail legal consequences, provides a testing ground for the potentially evolving international law.

105. Practical application of the recommendations of responsible behaviour of States as a means of regulating international relations can be an important step towards strengthening security in the context of use of ICT by States.

106. Voluntary application of recommendations of responsible behaviour of States can be achieved in the form of bilateral, multilateral, regional agreements and agreements of a universal nature. This goal can be supplemented with the necessary national normative-legal acts establishing the procedure for the application of voluntary norms, rules and principles of responsible behaviour of States in ICT environment.

Comment by the experts of the Cyber Policy Institute, The ICT4Peace Foundation, supported by the experts of the EastWest Institute

It is not often that the Western scholars get to work with their Russian colleagues on issues of international information or cyber security. It is unfortunate as the lack of contacts makes it difficult to find ways forward in the climate of political differences and competing world views.

We have found our cooperation with the Russian colleagues extremely informative and useful as it has helped us understand the Russian positions and views on several contested issues. We entered this project at the invitation of the International Information Security Research Consortium, Moscow State University to better understand how our col-

leagues approach the issue of implementing the norms, rules and principles of responsible state behavior as outlined in the UN GGE report of 2015.

At the end of this project, we can conclude that there are not only political but also fundamental methodological differences in how the Western and Russian scholars approach non-binding norms and international law. These differences make it close to impossible for the western colleagues to acknowledge and appreciate the proposals made by the Russian colleagues on how to implement the UN GGE recommendations and make them universally accepted. Whether there is agreement to be found on these differences or not, we consider it necessary to highlight these differences to facilitate finding consensus and ways forward in the international cybersecurity/information security discourse.

Experts in this very small group remained divided in three fundamental questions –

1) the relevance of the existing international law and current state practices to provide guidance on state behavior. The Russian colleagues are much more pessimistic about the susceptibility of existing rules and standards of international law to be usefully applied to issues of cybersecurity without progressive development. Based on our experience and expertise, we consider it possible to apply the rules and standards of existing international law, such as the prohibition of intervention or the obligation of peaceful settlement of international disputes, to issues of international cybersecurity. It would, indeed, require dialogue between states as to how to best interpret and implement these rules and standards.
2) the nature of the 2015 UN GGE report recommendations for norms, rules and principles for responsible state behavior. In the Russian conception, these norms, rules and principles will be implemented only after they acquire the legally binding status, either by state practice or treaty negotiation. From our perspective, the UN GGE recommendations can be implemented partially on the basis of existing international law and partially by way of national legislation and policy, which, as the Russian colleagues point out, constitutes the exercise of sovereignty.
3) the relevance of the question of attribution in the three examined GGE recommendations. Differences on attribution are particular to strategic contestants and, between these States, have raised concerns of less than satisfactory implementation of international law. For most of the States, however, attribution remains a still to be developed capacity and capability. Therefore, it is early to conclude whether the issue of attribution is, indeed, an equally significant issue of international law for the international community, or will the improvements and increase in national resilience and capacity resolve this issue in practice.

These divisions are also some of the key issues in the political negotiations that have taken place globally and bilaterally. Therefore, we conclude that successful and global implementation of the recommended norms is unlikely before nations come to agreement of their relevant premises and assumptions.

Most importantly, given these foundational differences, expert exchange, joint academic research and political dialogue must continue. This interaction should also cross disciplinary borders and involve more scholars and experts. Remaining in our trenches will only keep the war of attrition going on.

Notes