Utopía y Praxis Latinoamericana
ISSN: 1315-5216
ISSN: 2477-9555
diazzulay@gmail.com
Universidad del Zulia
Venezuela

Organization for Defense and Cooperation in the Field of Collective Cyber Security in Europe

ABDULLIN, ADEL ILSIYAROVICH; DAVLETGILDEEV, RUSTEM SHAMILEVICH; KOSTIN, SERGEY ANDREEVICH

Organization for Defense and Cooperation in the Field of Collective Cyber Security in Europe
Utopía y Praxis Latinoamericana, vol. 25, no. Esp.12, 2020
Universidad del Zulia, Venezuela
Available in: https://www.redalyc.org/articulo.oa?id=27965040013
DOI: https://doi.org/10.5281/zenodo.4280100

Artículos

Organization for Defense and Cooperation in the Field of Collective Cyber Security in Europe

Organización para la defensa y cooperación en el ámbito de la seguridad cibernética colectiva en Europa

ADEL ILSIYAROVICH ABDULLIN
Kazan Federal University, Rusia
adel.abdullin@kpfu.ru
https://orcid.org/0000-0001-6078-8029

RUSTEM SHAMILEVICH DAVLETGILDEEV
Kazan Federal University, Rusia
roustem.davletguildeev@kpfu.ru
https://orcid.org/0000-0001-5412-9027

SERGEY ANDREEVICH KOSTIN
Russian New University, Rusia
skostin@rosnou.ru
https://orcid.org/0000-0003-4114-4062

DOI: https://doi.org/10.5281/zenodo.4280100
Redalyc: https://www.redalyc.org/articulo.oa?id=27965040013

Received: 17 September 2020
Accepted: 07 November 2020

Abstract:

The paper analyses the activities of the Organization for Security and Cooperation in Europe (OSCE), which, as a result of the transformation of the Conference on Security and Cooperation in Europe (CSCE), has become one of the main elements of the European security architecture. The subject of interest is the international legal cooperation of the participating States in the field of international legal provision of the collective cybersecurity. Since its beginning the twenty-first century has been marked by the rapid development of information and communication technologies (ICT), which significantly accelerated communication processes both at the national and international levels.

Keywords: Cyber security, cyber space, international legal provision of collective security, Organization for Security and Cooperation in Europe (OSCE)..

Resumen:

El documento analiza las actividades de la Organización para la Seguridad y la Cooperación en Europa (OSCE), que, como resultado de la transformación de la Conferencia sobre Seguridad y Cooperación en Europa (CSCE), se ha convertido en uno de los principales elementos de la arquitectura de la seguridad europea. El tema de interés es la cooperación jurídica internacional de los Estados participantes en el ámbito de la disposición jurídica internacional de la ciberseguridad colectiva. Desde sus inicios el siglo XXI ha estado marcado por el rápido desarrollo de las tecnologías de la información y la comunicación (TIC), lo cual aceleró significativamente los procesos de comunicación tanto a nivel nacional como internacional.

Palabras clave: Ciberespacio, ciberseguridad, provisión legal internacional de seguridad colectiva, Organización para la Seguridad y la Cooperación en Europa (OSCE)..

INTRODUCTION

The Conference on Security and Cooperation in Europe was an unparalleled geopolitical project, the successful implementation of which made it possible to remove the critical international tension that existed at that time in matters of international security. Such an ambitious and far-reaching goal of this project became the basis for the transformation of the CSCE into the OSCE.

The Helsinki Final Act (the Final Act, or the Act) formulated the concept and direction of international cooperation through the "system of "three baskets": the military-political block; economic cooperation; humanitarian direction, and cooperation in the field of human rights" (Act: 1975, pp.323-325). Until a certain point in time, the concept of "three baskets" met the current requirements of the world order. However, against the background of the rapid desynchronized economic and technological development of states in the world, as well as a significant increase in the dependence of state bodies and enterprises on information technology, the international legal structure has come to an active state (Bakker&Kessels: 2012).

Recognizing the importance and dependence of international legal cooperation on ICTs, the United Nations (A/RES/57/239) was asked at the turn of the century to "create a global culture of cybersecurity" (Dunn&Mauer: 2006, pp.189-206), which, obviously, was to spread everywhere through regional international legal models. We will talk in this study about one of such international legal forms of relations within the frameworks of OSCE.

METHODOLOGY

The materials used in the work are international treaties, resolutions and decisions of international organizations, official statements by heads of states, as well as doctrinal studies related to ensuring international and regional security, namely its "cyber" component.

The methodological basis of the study is the special legal, normative, teleological and systematicinterpretation of international treaties, general scientific, as well as special scientific methods of cognition characteristic of legal sciences, including logical, formal legal, etc.

RESULTS

In the period from July 1973 to August 1975, a number of meetings on security and cooperation in Europe were held. They resulted in the removal of tensions in matters of security in the European region, which were associated, in particular, with the strengthening of revanchist sentiments. The meeting resulted in the signing of the Helsinki Final Act. In the section of the Act "related to security in Europe", ten principles of international law "jus cogens" were formulated on which the doctrine of international law is based. The Act also reflects the concept of development and cooperation based on the principle of "three baskets": the military-political area of relations; cooperation in the economic and humanitarian fields, and in the field of human rights protection.

As a result of the rapid ICT development and the emergence of a new type of space, i.e. cyberspace, the world community faced a number of challenges related to maintaining the required level of security. The key ones are the transboundary aspect of cyberspace and the lack of uniformity of international legal regulation of relations in cyberspace. Referring to a number of authors, D.V. Krasikov draws attention to the fact that:

> Currently there is, on the one hand, the 'territorialization' of cyberspace, i.e. the spread of such a configuration of power to it, which acts in relation to territorial spaces, and on the other, its "deterritorialization" in the sense of recognition and development of extraterritorial jurisdictionalapproaches limited by the current international law, but needing to be clarified taking into account the specifics of activities in cyberspace (Krassikov: 2018).

According to the interactive map of cyber threats developed by Kaspersky Lab, the OSCE participating States constitute the absolute majority as a percentage of both the total number of "infections" of countries in the world and the total number of cyber-attacks (Baykara et al.: 2018, pp.1-6) in terms of the volume of "infections". P.L. Pilyugin draws attention to the fact that:

> The state should be responsible for criminal acts committed from its territory; it should have the ability to prevent or suppress such actions. Within the existing transport systems, a state, as a rule, is able to regulate and control both the communication

> routes, and the equipment that provides them, and the companies operating them, as well as filter traffic at their borders (customs, passport control, anti- terrorist control, veterinary control, etc.). This practice has not yet developed in relation to the global network. (Pilyugin&Salnikov: 2016)

The transboundariness problem can be partially resolved through the conclusion of international bilateral agreements, such as, for example, the 2013 "Agreements on Confidence Building Measures in the Use of ICTs" between the Russian Federation and the United States of America (Clinton& Putin: 2000) or bilateral agreements related to security in the sphere of using ICT. However, what about states that are not bound by bilateral international legal obligations in this area of relations? The answer is unequivocal: to overcome the negative aspect of the transboundary nature of cyberspace by becoming part of a single integration contour of the global institutional system.

The OSCE as an interregional organization, which competence includes security issues, has the broadest representation of states in comparison with any other regional international organization. This allows for the coordination of crime prevention activities in a broader international format. Paragraph 22 of Decision No. 1063 states that "the Anti-Terrorism Unit of the Department for Transnational Threats (ATU UTTD) will continue to act as a coordinating centre, information resource, and partner in the practical implementation of OSCE counter-terrorism activities" (Billen: 2005). Such an advantage should be used both in the framework of the coordination of international anti-terrorist activities and in other areas of the "interdimensional aspects" of OSCE activities, in which the transboundary aspect of cyberspace is a significant negative element.In 2012, ATU UTTD held a "Series of expert online forums on the use of the Internet by terrorists: threats,responses, and possible future steps". Its experts noted that:

> The Internet and the ever-growing number of tools to access it have given terrorists a potential tactical advantage never seen before the emergence of the Internet ... that terrorists are already turning to other cybercriminals to develop their own skills, and this trend is likely to continue in the future ... The lack of a harmonized legal system may exacerbate the existing difficulties associated with international cooperation (Gill et al.: 2017, pp.99-117).

I.M. Rassolov rightly believes that "it is more expedient to introduce a legal framework based on collective interaction and general consent, implying voluntary acceptance and implementation of legal norms" (Rassolov: 2016). However, over time, no significant progress has been observed in resolving this issue in the international legal plane.

Another important area is highlighted in the context of interdimensional threats in the use of information and communication technologies (ICT); this area is international legal terminology. By Decision of the OSCE Permanent Council No. 1039 dated April 26, 2012, it was ordered "to develop a draft set of confidence and security-building measures (CSBMs) in order to increase interstate cooperation, transparency, predictability and stability, and reduce the risks of misperception, escalation and conflicts that may arise due to use of ICT"(Borghard&Lonergan: 2018, pp.10-49). Paragraph 9 of the OSCE Permanent Council Decision No. 1106 dated 03 December 2013 states that with the aim of

> Reducing the likelihood of misunderstandings in the absence of agreed terminology and facilitating the continuation of the dialogue, the participating States will, as their first step, provide on a voluntary basis a list of ICT security terms they use, accompanied by an explanation or definition for each term. Each participating State will select on a voluntary basis those terms that are most appropriate to them for exchange. The participating States will try to draw up a glossary agreed by consensus in the longer term. (Dincă: 2019, pp.225-234)

In the context of terminology, and in addition to this Decision, the OSCE Permanent Council Decision No. 1202 dated March 10, 2016 has proposed "the adoption on a voluntary basis of national systems for classifying ICT incidents according to their scale and severity" (Ackermann: 2012, pp.223-233). Professor A.A. Streltsov proposes to consider "clarification of the terminology of international conflict prevention law in relation to cyberspace (the rules of responsible behaviour of states in cyberspace" (Streltsov: 2016) as one of the main directions for adaptation of international security law to ICT.

DISCUSSION

To date, there is no any generally accepted definition of the "cyberspace" concept in the international legal doctrine. Various formulations are offered from the most general ones, such as “cyberspace is a virtual world, the space of computers, servers, modem and the Internet” (Teitel: 2016) or “cyberspace is a transnational sphere of information technology infrastructures and interdependent networks. It includes the Internet, telecommunications networks, computer systems and embedded processors in critical industries" (Brannon& Centre: 2014), to more specific "cyberspace is an artificially created environment consisting of geography, hardware, logical networks (software, applications), and user profiles (usernames and their logins), as well as people" (Alexander&Jaffer: 2018, pp.51-66).

It should be noted that all the proposed formulations have something in common: this is the environment in which communications are carried out using ICT. However, these definitions can hardly be called legal, since they do not contain references to either the subject of the relationship, or the object and the objective side in which the relationships are expressed, or, finally, about the subjects. Despite this, it is obvious that the objective side of interaction in cyberspace is expressed in a complex of actions of subjects using software and hardware tools and ICT, the result of which has or may have expression, i.e. entails or may entail legal consequences. In CSBMs developed in the OSCE format, one of the main tasks is the development of uniform standards in ICT terminology.

Transboundariness is becoming a challenge both from the point of view of maintaining the required level of security, and from the point of view of defining the international legal regime of cyberspace. In its internal information and transport systems, a state provides regulation and control of information interaction, including by means of controlling the appropriate organizations and institutions that own the relevant IT equipment. However, such a practice has not developed yet in the interstate format with regard to the global network. In his speech at the OSCE Permanent Council in Vienna, Daniel Baer drew the attention to the fact that “we are witnessing more and more sophisticated cyber-attacks that are global in nature and which are almost impossible to trace back to the source” (Kemp: 2016). In turn, speaking at the OSCE international conference on cybersecurity on November 3, 2017 in Vienna, the Deputy Secretary of the Security Council of the Russian Federation O.V. Khramov rightly noted that “given the practical impossibility of reliably identifying the sources of computer attacks, we believe that this approach actually legalizes the possibility of conducting not only information, but also military operations against ”inconvenient states” (Zellner: 2005, pp.389-402). Theemergence of international bodies whose competence would be to investigate cases of crimes using ICTs and to prosecute those responsible in court, not limited to the principle of territoriality, would significantly contribute to the solution of these tasks, and the OSCE format, in this context, can be effectively used to make relevant decisions.

Currently, the OSCE does not have independent institutions that would deal with the problems of preventing acts of international terrorism using information and communication technologies. The OSCE open- ended working group created under the auspices of the Security Committee on the basis of the OSCE Permanent Council Decision No. 1039 dated April 26, 2012, is informal, which does not correspond to current realities. The issue of formalizing the actions of the working group may well be resolved by expanding the functions and competence of the OSCE Anti-Terrorism Unit of the Transnational Threats Department, which will help clarify the internal organizational mechanism of the OSCE's work and distribute its competence among the existing institutions.

CONCLUSION

The CSCE was convened for the purpose of dialogue, coordination of foreign policies of states, and the development of constructive solutions for cooperation. With the passage of time and with the development

of information and communication technologies, threats requiring interstate regulation have transformed. However, by that time the OSCE had become one of the main system-forming elements in the international legal architecture of European security. Academician A.G. Arbatov rightly notes that:

> The former leaders of the great powers were convinced of this from their own hard experience, and their current generation, apparently, will have to repeat this path, if it would not be interrupted by a global catastrophe. In the past, ending the arms race and ending the Cold War required great and long-term efforts by the ruling circles and the concerned public in the USSR, the United States, and other countries. Henceforth, the restoration of the arms control system will require no less political and intellectual investments from the responsible powers of the world (Arbatov: 2020).

The development of ICTs has predetermined the emergence of complex international legal issues, the solution of which is possible only through an equal dialogue of states, based on the principles of international law uniting most states of the world community.

The OSCE has every chance to become a specialized international organization being a universal institutional contour, with clear rules for the international legal regulation of relations in cyberspace. The OSCE participating States are able to develop clear rules for the international legal regulation of relations in cyberspace and unite the participating States under its own international legal framework, thereby reducing the "blank spots" on the digital map of cyberspace.

Acknowledgements

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

BIODATA

A.IABDULLIN: Professor, Doctor of Legal Sciences. Research interests: international private law, international public law, European law. He is the head of the Department of International and European Law at Kazan (Volga Region) Federal University. Author of numerous scientific and educational works.

R.S DAVLETGILDEEV: Associate Professor, Doctor of Legal Sciences. Research interests: international law, international labour and migration law, theory of legal integration. He is the head of the Department of Theory and History of State and Law at Kazan (Volga Region) Federal University. Author of numerous scientific and educational works.

S.A KOSTIN: Candidate of Legal Sciences. Research interests: international law, international security law. He is the executive director of the Law Institute of the Russian New University. Author of a number of scientific works.

BIBLIOGRAPHY

ACKERMANN, A (2010). "OSCE mechanisms and procedures related to early warning, conflict prevention, and crisis management." In OSCE Yearbook, pp.223-233.

ACT, HF (1975). "Conference On Security And Co--Operation In Europe." DEP'T ST. BULL., 73(21), pp.323- 325.

ALEXANDER, GKB & JAFFER, JN (2018). "Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition." Georgetown Journal of International Affairs, 19(2), pp.51-66.

ARBATOV, AG (2020). New technological factors and the future of the arms control system.

BAKKER, E & KESSELS, E (2012). "The OSCE's Efforts to Counter Violent Extremism and Radicalization That Lead to Terrorism: A Comprehensive Approach Addressing Root Causes." Sec. & Hum. Rts., 23(12).

BAYKARA, M, GURTURK, U& DAS, R (2018). "An overview of monitoring tools for real-time cyber-attacks." In 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp.1-6.

BILLEN, C (2005). The OSCE: a platform for co-operative counter-terrorism activities in Central Asia? Institute for Peace Research and Security Policy at the University of Hamburg/IFSH (ed.), OSCE Yearbook.

BORGHARD, ED & LONERGAN, SW (2018). "Confidence Building Measures for the Cyber Domain." Strategic Studies Quarterly, 12(3), pp.10-49.

BRANNON, RB & CENTRE,DM (2014). "A comprehensive non-technical program on cybersecurity for officials and professionals." Journal on the problems of security and defence in Europe Per Concordiam,5(2).

CLINTON, WJ & PUTIN, V (2000). Joint Statement By The Presidents Of The United States Of America And the Russian Federation On Principles Of Strategic Stability.

DINCĂ, CF (2019). "OSCE WORK ON CONFIDENCE BUILDING MEASURES IN CYBERSPACE: ACCOMPLISHMENTS, CHALLENGES AND POTENTIAL FUTURE EVOLUTIONS." In International ScientificConference" Strategies XXI", 1(5), pp.225-234.

DUNN, M &MAUER, V(2006). "Towards a Global Culture of Cyber-Security." The International CIIP Handbook, 2(7), pp.189-206.

GILL, P, CORNER, E, CONWAY, M, THORNTON, A, BLOOM, M & HORGAN, J (2017). "Terrorist use of theInternet by the numbers: Quantifying behaviors, patterns, and processes." Criminology & Public Policy, 16(1), pp.99-117.

KEMP, W (2016). OSCE peace operations: soft security in hard environments. Walter Kemp,"OSCE Peace Operations: Soft Security in Hard Environments," New York: International Peace Institute.

KRASSIKOV, DV (2018). Territorial sovereignty and delimitation of jurisdictions in cyberspace.

PILYUGIN, PL&SALNIKOV,AA (2016). Prospects for the application of international legal norms in cyberspace. Information and analytical portal DigitalReport.

RASSOLOV, IM (2016). Law and Cyber Space. Monograph. - 2nd edition - Moscow: Moscow Bureau for Human Rights.

STRELTSOV, AA (2016). Adaptation of international security law to the information space. Information and analytical portal DigitalReport.

TEITEL,R (2016). "Definition of the concept of cyber terrorism." Journal on security and defence of Europe Per Concordiam, 7(2)

ZELLNER, W (2005). "Russia and the OSCE: From high hopes to disillusionment." Cambridge Review of International Affairs, 18(3), pp.389-402.