ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 105

1st International Scientific and Practical Conference on Digital Economy (ISCDE 2019)

Safeguarding of critical digital infrastructures

Shinkaretskaya G.G.
Institute of State and Law
of the Russian Academy of Sciences
Moscow, Russia
gshink@yandex.ru

Lyalina I.S.
Institute of State and Law
of the Russian Academy of Sciences
Moscow, Russia
irlyalina@yandex.ru

***Abstract*—The paper deals with the legal regulation of safeguarding of critical digital infrastructures at the national and international levels. Particular attention is paid to issues of cooperation between countries to protect critical infrastructures within the framework of the United Nations and its specialized agencies and bodies, regional international organizations, informal international bodies and forums. The authors note that the new rules governing the safety of critical infrastructures appear in the form of "soft law", they are not included in the treaties, and many of them represent a modification of the existing norms of international law. It is concluded that the existing provisions of general international law can be applied to regulate digitization and, in particular, the security of critical infrastructure, subject to special interpretation and additional measures.**

***Keywords*—digitization, international law, information, information law, infrastructure, security, cybersecurity.**

I. INTRODUCTION

The spread of information technology in all areas of human life has its positive and negative sides. Computer networks make it possible to quickly obtain the information necessary for both work and entertainment. However, these same computer networks practically eliminate any secrets, or, in any case, greatly facilitate access to them. Therefore, one of the pressing problems of our time is the security of infrastructures [1].

The threat to their security can come from two sides—within the State itself from criminal elements and from other States as an expression of their hostile attitude.

Digitization gives criminals or hostile countries new, unprecedented means of warfare and the seizure of foreign territories. The fact is that digitization means the introduction of computer control in the most diverse areas of our lives: transport, energy, life support systems of settlements, which makes these systems easily susceptible to destruction. An intrusion of a hacker, let's say, into a power supply system allows to disable an entire city or industrial enterprise, or defense complex. Thus, the computer system itself becomes a powerful time bomb.

II. MAIN PART

A concept has emerged for which there is no established term. This is the concept of a complex that makes up a complex system that ensures the functioning of the whole system and which is controlled by a computer. Its most characteristic feature is that such infrastructure is easy to destroy, which is why they are called sensitive infrastructures.

These properties of infrastructures are reflected in Federal Law No. 187 [2], where Article 2 gives an interpretation of several parameters of the regulated phenomenon: "automated control system", security of critical information infrastructure, significant object of critical information infrastructure, computer attack, computer incident, critical information infrastructure, objects of critical information infrastructure, and subjects of critical information infrastructure.

The US law, starting with the USA PATRIOT Act of 2001, invariably understands critical infrastructure as both physical and virtual systems and assets so vital to the United States that the failure or destruction of such systems and assets will have a devastating effect on security, national economic security, national health and safety, or any combination of these factors [3].

The Executive Order of the President of the United States on *Improving Critical Infrastructure Cybersecurity* of 2013 [4] emphasizes the importance of the reliable functioning of the critical infrastructure of the State for national and economic security, and the critical infrastructure sectors include, in particular: water supply and other communications, transport, energy, information technology, chemical industry, defense industry, financial sector, agriculture, medicine, nuclear energy, government, and emergency services.

The critical national infrastructure of the United Kingdom of Great Britain and Northern Ireland consists of the same facilities, systems, information objects, people, networks, and processes necessary for the functioning of the country and on which everyday life depends. Also, objects requiring protection due to their potential danger can be attributed to it. Currently, the main sectors of critical national infrastructure are: chemical industry, nuclear energy, communications, defense, rescue services, energy, finance, food, government, healthcare, space, transport, and water [5].

Within the European Union, there is the Directive of the European Parliament and of the Council of 2016 concerning measures for a high common level of security of network and information systems across the Union [6], which establishes a set of criteria for identifying operators of these critical (basic) services: the service provided is necessary to maintain critical social and (or) economic activity; the provision of this service depends on the network and information systems; an accident, that is, any event that has a real negative impact on the

security of network and information systems and which will have serious destructive consequences for providing this service.

The Directive defines such critical sectors as energy, transport, banking and financial market infrastructure, healthcare, drinking water supply and water distribution, and digital infrastructure.

The legal regulation of individual Members of the European Union as a whole reflects this approach, supplementing it with government, court proceedings, and defense that is critical for any country. This is reflected, for example, in the German *Law on Information Security* [7] and the *Regulation* defining critical infrastructures in accordance with this law [8], as well as in French legislation [9].

Due to the fact that each State, depending on various kinds of reasons, understands in its own way and sets the criteria and lists of objects related to critical infrastructure, it is hardly possible in principle to expect a unified at a universal level approach in this area in the coming years. However, within the framework of regional integration associations, the development of uniform rules in this area seems promising.

The laws of different countries have formed some common approaches to curbing the crime of hacking and mainly criminal measures are being taken. Moreover, some other measures are being taken. These measures have a threefold focus:

- protecting infrastructures from criminal attacks;
- creation of a special protection regime for "hazardous" materials;
- the creation of flexible systems to counter the destructive power of attacks and eliminate their consequences [10].

Critical infrastructures are at the center of any information security regulation. Prior to the Manhattan terrorist attack, the importance of protecting infrastructures was generally recognized [11]. After this attack, legislative measures became more specific [12]. The issues of protecting information infrastructures also began to be addressed by the Counter-Terrorism Committee established by the Security Council [13]; this issue did not go unnoticed by the Organization for Security and Co-operation in Europe [14].

A notable phenomenon in the legislation of recent years has been measures that are not specifically tailored to the fight against terrorism; this allows not engaging in categorization in order to prevent threats to sensitive infrastructures. In other words, the source of danger is not of great importance for strengthening the security of such structures. This is reflected in international documents [15].

If the application of criminal law to attacks on infrastructures, which is most often used in national legislation, involves a so-called reactive approach, that is, retaliatory measures, a specific act, then international law most likely approves an approach based on "due diligence", which allows reducing the possible harmful effects of the attack [16].

The concept of "due diligence" is used throughout the State in relation to foreign investment and human rights. In international relations, such obligations can be found in environmental law: there is a State obligation to take measures to prevent such actions within its jurisdiction that could harm another State. International law in the protection of economic, social, cultural rights requires States to protect such rights from violations by non-States, for example, corporations. In this regard, one can also raise the question of the obligation of legal entities to abide by the establishment of international law, which has not yet been resolved and not even properly posed in the Doctrine [17].

Elements of the concept of "due diligence" can also be found in the rules formulated by the International Telecommunication Union. Its Constitution [18] requires Member States to support, provide, and guard against violations of channels and technical devices that provide global communications [19]. These provisions are of particular importance for ensuring the priority of telecommunications, which are important for saving human life at sea, on land, and in space, and for urgent communication of WHO in the fight against epidemics. The ITU Constitution also contains Member States' commitments to prevent malicious interference with radio services.

It is also worth noting the role of ITU in the development of digitization and countering cyberthreats, which are currently the most important areas of activity of this international organization. ITU not only participates in discussions at the global and regional level, but also assists the States in developing national cybersecurity strategies of States [20], as well as in creating and improving the effectiveness of National Computer Incident Response Teams (CIRTs)).

It should be recognized that so far there are not very many legal norms in international law specifically related to the protection of critical infrastructures, but there are grounds for the formation of such provisions.

Specific standards regarding the protection of critical infrastructures are formulated by lawmakers for application within States on the basis that they are able to implement such protection without resorting to international mechanisms, international cooperation, and international law. Nevertheless, there are more and more cases of international contacts in this area in the practice of the States.

So far, the recognition of the importance of cooperation regarding the protection of critical infrastructures is more often found not in international treaties, but in documents of informal international bodies, such as, for example, the UN Expert Group on Telecommunications Security [21]. Similar conclusions are in the documents of regional organizations: ASEAN [22], European Union [23], and Organization of American States [24]. Attention is paid to the security of infrastructures and such an influential international, albeit informal organization, as the Organization for Economic Cooperation and Development (OECD). In the Declaration drawn up within the framework of this organization, Member States announced their readiness not only to contribute to digital security risk management and privacy protection, but also to strive to develop and adopt agreed digital security

strategies [25].

We can also name organizations that have security as their primary goal: NATO [26] and the Shanghai Cooperation Organization [27]. Similar informal documents are found in bilateral international relations [28].

In April 2015, more than forty countries held the so-called Global Forum on Cyber Expertise (GFCE) to discuss potential collaboration in improving the digitization of the global economy [29]. One of the issues discussed at the Forum was the issue of involving all countries, including developing ones, in the process of ensuring the safety of information telecommunications [30]. The importance of universal participation, including developing countries, is emphasized in the reports of the UN Group [31].

Thus, for several decades, the practice of digitization in various countries seemed to prove that there is no need to formulate new rules of international law to regulate activities and protect information infrastructures. States are resorting to improving their own digitization policies. This situation is reminiscent of the situation with the use of nuclear materials [32], transboundary pollution [33], industrial incidents [34], where the emphasis is on security operations, the dissemination of information, assistance, as well as on the development of cooperation to improve the protection of critical infrastructures.

III. DISCUSSION

Indeed, existing international law turned out to be flexible enough to protect critical information structures using norms that do not have such a specific focus. A rather unexpected trend appeared—international organizations specializing in other areas began to deal with the problems of digital infrastructures.

The Department for Nuclear Safety and Security of the International Atomic Energy Agency (IAEA) adopted the Computer and Information Security Program [35], and during the Sixth Conference on the Review of the Convention on Nuclear Safety, cybersecurity was identified as an urgent problem [36]. The International Civil Aviation Organization (ICAO) addressed a number of cybersecurity issues and included some recommendations related to the prevention of cyberattacks on critical infrastructures in the Annex on air safety to the Convention on Civil Aviation [37]. The Facilitation and Maritime Safety Committees of the International Maritime Organization (IMO) have initiated a review of information security issues [38]. Another IMO committee, namely the International Cable Protection Committee, also began to include relevant issues on its agenda [39]. The UN Security Council drew the attention of Member States to the need to take measures in order to protect critical infrastructures when implementing its resolutions [40].

There are not so many international law provisions specifically related to the protection of digital infrastructures. Among the organizations that paid attention to this, the European Union should be mentioned first of all. The most common document is the Council Directive, which requires Member States to identify European critical infrastructures in the field of energy and transport, to provide information on the composition of such infrastructures and plans for ensuring their safety [41].

The members of the Shanghai Cooperation Organization agreed to carry out cooperation “to ensure the information security of critical structures” [42].

Adopted by Members of the African Union, but not yet in force, the AU Convention on Cybersecurity and Personal Data Protection provides that Member States will determine the direction of national policy, which includes measures to protect critical infrastructures and toughening penalties for criminal acts against such infrastructures [43].

Currently, it notes the emergence of new standards that specifically regulate the safety of critical infrastructures. However, such standards appear most often in the form of “soft law”, because they are not included in the contracts. Most of them are modifications to existing provisions of international law adapted to protect critical infrastructures, such as the rule that States should refrain from intentionally damaging the infrastructures of another State, which was included in the 2015 UN Group report [44]. It is clear that this rule is based on the principles of sovereignty, non-interference in internal affairs, and the non-use of force [45].

IV. CONCLUSIONS

Thus, modern international law contains provisions that can be the basis for the formation of special rules governing the security of critical information infrastructures. And this is actually a process of applying the norms of general international law to the specific context of digitization: it means that these are not new norms, and their application requires additional interpretation. Therefore, a number of additional measures are needed to build a consistent and effective system of legal norms.

Furthermore, an urgent problem is the regulation of the behavior of legal entities and individuals, which are often denoted by the term “non-state actors”. It is individuals and legal entities that often act as operators of digital infrastructures, and thus are responsible for their safety. From this point of view, the question arises of the presence or absence of obligations created by international law for individuals and legal entities.

Acknowledgment

The study was carried out with the financial support of the RFBR in the framework of the scientific project No. 18-29-16012.

References

[1] Polyakova T.A. Tsifrovizatsiya i sinergiya pravovogo obespecheniya informatsionnoy bezopasnosti // Informatsionnoye pravo. 2019. № 2 (60). S. 4-7.

[2] Federal'nyy zakon ot 26.07.2017 N 187-FZ "O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii"

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. H.R.3162 // https://www.congress.gov/bill/107th-congress/house-bill/3162/text?overview=closed&r=9

[4] Executive Order - Improving Critical Infrastructure Cybersecurity // https://obamawhitehouse.archives.gov/the-press-

office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[5] Public Summary of Sector Security and Resilience Plans 2018 // https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[7] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) // https://www.bgbl.de/xaver/bgbl/start.xav?start=//*%5B@attr_id=%27bgbl109s2821.pdf

[8] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf

[9] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) // https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s 0958.pdf

[10] Instruction generale interministerielle relative a la securite des activites d'importance vitale, 7 janvier 2014 // http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf

[11] David P. Fidler. Whither the Web? International Law, Cybersecurity, and Critical Infrastructure Protection // Georgetown Journal of International Affairs (2015). P. 8-20.

[12] Presidential Decision Directive/NSC-63, Critical Infrastructure Protection, May 22, 1998.

[13] U.S. Office of Homeland Security, National Strategy for Homeland Security (July 2002); White House, National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Feb. 2003).

[14] Counter-Terrorism Committee, CTED Stresses Need to Protect Critical Infrastructures, Mar. 23, 2015, http://www.un.org/en/sc/ctc/news/2015-03-23_cted_protect_infrastructure.html.

[15] Organization for Security and Co-Operation in Europe, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace (2013).

[16] Convention on the Marking of Plastic Explosives for the Purpose of Detection, Mar. 1, 1991, entered into force June 21, 1998, 2122 UNTS 359; UN Security Council, Resolution 1540 (2004); Konventsiya o bor'be s bombovym terrorizmom; Konventsiya o fizicheskoy zashchite yadernogo materiala. Mar. 3, 1980, entered into force Feb. 8, 1987, 1456 UNTS 124; Arms Control Association, Nuclear Security Summit at a Glance, Apr. 2014, http://www.armscontrol.org/factsheets/NuclearSecuritySummit.

[17] Duncan French and Tim Stephens, Due Diligence in International Law (First Report of ILA Study Group on Due Diligence in International Law, Mar. 7, 2014).

[18] Шинкарецкая Г.Г. Новые действующие лица в международном праве // Материалы юридического форума «Россия-Турция. XXI век». М., 2011. С.15-24

[19] Constitution of the International Telecommunication Union // https://www.itu.int/council/pd/constitution.html

[20] ITU Constitution, in Collection of the Basic Texts of the International Telecommunication Union // https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

[21] Framework for Improving Critical Infrastructure Cybersecurity, 4. 294 GGE Report (2013), 26(e); GGE Report (2015) 13(h).

[22] Caitríona H. Heinl, Regional Cyber Security: Towards a Resilient ASEAN Cyber Security Regime (RSIS Working Paper No. 263, Sept. 9, 2013), http://www.rsis.edu.sg/wp-content/uploads/rsis-pubs/WP263.pdf

[23] European Commission, Critical Infrastructure, http://ec.europa.eu/dgs/home-affairs/what-wedo/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm. 297

[24] OAS, Critical Infrastructure Protection Programs: Cyber Security, http://www.oas.org/en/sms/cicte/programs_cyber.asp; Inter-American Committee against Terrorism, Declaration on Protection of Critical Infrastructure from Emerging Threats, Mar. 20, 2015, OEA/SER.L/X/2/15 & CICTE/doc.1/15, Mar. 23, 2015.

[25] Ministerial Declaration on the Digital Economy: innovation, growth and social prosperity ("Cancún Declaration"), Jun.23, 2016. // https://www.oecd.org/internet/Digital-Economy-Ministerial-Declaration-2016.pdf

[26] Critical Infrastructure Protection (Matthew Edwards ed.) (NATO Science for Peace and Security Series Vol. 116) (Amsterdam: IOS Press, 2014).

[27] Agreement on Cooperation in the Field of International Information Security, June 16, 2009, https://ccdcoe.org/sites/default/files/documents/SCO-090616IISAgreement.pdf.

[28] Canada-United States Action Plan for Critical Infrastructure (2010), http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf.

[29] The Global Conference on Cyberspace: Putting Principles into Practice. // http://2007-2017-blogs.state.gov/stories/2015/04/30/global-conference-cyberspace-putting-principles-practice.html

[30] GFCE, Report of International Kickoff Meeting 2 & 3 November 2015 (Nov. 15, 2015), 10-11.

[31] GGE Report (2015), P. 19-23.

[32] Convention on Nuclear Safety, Jun. 17, 1994, entered into force Oct. 24, 1996.

[33] Convention on the Law of the Non-Navigational Uses of International Watercourses, May 21, 1997, entered into force Aug. 17, 2014, UN Doc. A/51/869.

[34] Convention on the Transboundary Effects of Industrial Accidents, Mar.17, 1992, entered into force Apr. 19, 2000.

[35] Oszvald Glöcker, IAEA Coordinated Research Project (CRP) on Cybersecurity of Digital I&C Systems in Nuclear Power Plants, May 26, 2011, http://www.iaea.org/NuclearPower/Downloadable/Meetings/2011/2011-05-24-05-26-TWG-NPPIC/Day3.Thursday/TWG-CyberSec-O.Glockler-2011.pdf.

[36] Sixth Review Meeting of the Contracting Parties to the Convention on Nuclear Safety, Summary Report, CNS/6RM/2014/11_Final, Apr. 4, 2014, 6.

[37] Convention on International Civil Aviation, Dec. 7, 1944, entered into force Mar. 5, 1947, ICAO Doc. 7300, Annex 17 (Security).

[38] IMO, Maritime Security, http://www.imo.org/en/MediaCentre/HotTopics/piracy/Pages/default.aspx.

[39] International Cable Protection Committee, ICPC Achievements, July 24, 2015, https://www.iscpc.org/about-the-icpc/achievements/ (reporting on ICPC Chairman's participation in the Worldwide Cyber Security Summit in 2013).

[40] Counter-Terrorism Committee, Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States, 64 (noting vulnerabilities facing critical infrastructure in the transportation sector of many states).

[41] Council of the European Union, Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection, Dec. 8, 2008, Official Journal of the European Union, L/345/75-L/345/81, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

[42] Shanghai Cooperation Organization, Agreement on Cooperation in the Field of International Information Security, Article 3.

[43] AU Convention on Cybersecurity and Personal Data Protection, Jun. 27, 2014, Article 24.

[44] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 // https://undocs.org/en/A/70/174

[45] Developments in the field of information and telecommunications in the context of international security //https://undocs.org/pdf?symbol=en/A/RES/73/27