VYTAUTO DIDŽIOJO UNIVERSITETAS
MCMXXII

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

CYBER THREATS AND GLOBAL BUSINESS ENVIRONMENT

Taras Tsymbrivskyy[1]
DOI: http://dx.doi.org/10.7220/2029-4239.16.2

SUMMARY

The paper deals with the issue of cyber threats within the realm of global business environment, approached through the multidisciplinary prism: law (national and international law), politics, economics, philosophy. Article's structure is divided into 4 parts. Introduction submits facts in order to demonstrate the authenticity of cyber threats and especially their large-scale damage suffered by global business entities. Current vulnerabilities of cyber domain are a consequence of its decentralized architecture and shortage of law regulations.

In the second part "Hybrid threats" brief notice is given of concept's essence, its interpretation with due regard to cyber threat as a form of hybrid threat. Specifically, the cyber attacks represent a type of hybrid threats, endangering the performance of states fundamental functions. Launching cyber attacks against critical infrastructure of states could give rise to the invocation of unilateral or collective self-defense, in line with the international law. Current applicability of contemporary international law to the cyber domain substantially diminishes the chances of new legal regime emergence.

The third part "Critical national infrastructure and legal framework" focuses on defining the notion of critical national infrastructure and respectively its disposure to cyber threats. Notwithstanding the fact that the notion of "critical national infrastructure" does not enjoy a uniform understanding, it is subject to the states determination by means of adoption national legislation.

Adversaries employ a number of sophisticated types of operations in the cyber space which presuppose distinct legal regulation and different resilience mechanisms. Resort to cyber attack, being one the gravest cyber threats, might even trigger the inherent right of states to self-defense. Nowadays the use of force could not be rendered to its classical but yet rather restrictive interpretation, namely referring just to the kinetic means. Cyber attacks exemplify a brand new type of use of force, employed by the adversaries in the international relations. Rapid

[1] Author is Ph.D, assoc. prof., Department of Theory of Law and Human Rights; Ukrainian Catholic University, Lviv, Ukraine. E-mail: tsymbrivskyy@ucu.edu.ua

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

developments in the field of digital environment substantially leave behind the existing legal regulations. Cyber threats are addressed in terms of cyber security measures undertaken on universal (UN), regional (EU, NATO) and national level. Bolstering cyber security should include artificial intelligence technologies.

Deficiency of one fits all approach towards enhancing cyber security requires seeking for the alternatives. Employment of an artificial intelligence within the cyber domain is worth considering among many options. Obvious advantages of artificial intelligence systems are usually followed by a number of risks. Undisputed benefits provided by the utilization of artificial intelligence in the field of cyber security should be assessed though the risks. The latter predominantly relates to the caveat against artificial intelligence transforming into a weapon possessing supernatural features. Promising future of artificial intelligence (managing complex systems combined with multitasking; likewise its opposite application with the aim of compromising other states), however not yet discovered to the full extent, is hard to resist. Hence, paving way for a future arms race between states. Key developments in the area of cyber security will be apparently influenced by the proliferation and subsequent sophistication of artificial intelligence systems.

Conclusions outline key findings of the research. Capacities of cyber threats have not been exhaustively disclosed by the adversaries and hence such an obscurity is even more dangerous than ever.

KEY WORDS

Anonymity, accountability, conduct attribution, globalization, digital environment, Internet, cyber domain, cyber security strategy, hybrid threats, jurisdiction, cyber attacks, cyber operations, cyber intrusions, malware, state and non-state actors, business entities, domestic law, international law, use of force, artificial intelligence, risk assessment, security vulnerabilities.

INTRODUCTION

Growing interconnectivity within the global dimension (economy, communications, cyber space) has immensely enhanced upon the advent of internet and exponential proliferation of new technologies henceforth. In accordance with the latest surveys as of 2017, world's penetration rate of internet makes 49,6 %[2]. By 2020 the expansion of devices will reach 200 billion[3].

Rising cyber dependency delineated among top trends influencing global developments[4].

[2] "Internet World Stats. Usage and Population Statistics" // http://www.internetworldstats.com/stats.htm

[3] "ACS. Cybersecurity. Threats. Challenges. Opportunities" (November, 2016) // https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

[4] World Economic Forum. "The Global Risks Report" (12th edition, 2017) // http://www3.weforum.org/docs/GRR17_Report_web.pdf

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

Notwithstanding a great many benefits (cheap and accessible technologies[5]) thus brought about, the digital environment in particular has become inherently vulnerable, highly prone to intrusions. Seemingly, our opportunities have been leveled by risks[6].

Apart from being a free marketplace and source of information[7], the cyber space has turned into a key rivalry domain[8] among a wide range of actors (states, not even necessarily rogue states, criminal networks, non-state actors, individuals[9] etc.). Cyber-attacks could introduce worrisome spill-over effects, leading to serious economic damage, geopolitical tensions or a widespread loss of trust in the internet[10]. Some of the recent incidents connected with invocation of cyber threats were alarming in terms of the peril gravity.

A feasible risk from cyber threats to global economy is indicative of malware dissemination. Alike exploitation of security vulnerabilities in computer systems endangers business environment relying heavily on such technologies. In 2001 virus Love Bug infected millions of computers and caused an estimated $10 billion in lost work hours of such businesses as Ford, Siemens, and Microsoft, as well as government departments of various countries[1112]. Also in 2005 Daimler Chrysler auto plants suffered considerable financial losses (around $14 million) as a consequence of attack of company's network by the virus Zotob[13].

In 2007 large scale DDoS cyber operations crippled websites of Estonia's media, government, banking sector[14], whereafter one of the Estonian banks reported about its operational losses estimated around $1 million in damage[15]. In addition to the above, in 2009 sophisticated Stuxnet virus infiltrated into Siemens control system incapacitated Iran's uranium enrichment centrifuges[1617].

Another worthwhile example here is Hezbollah which by virtue of cyber operations targeted at Israel's official and financial websites disrupts its economy and disables servers used for e-

[5] Prime Minister's Office Publications. Government report on Finnish Foreign and security policy. (9/2016) // http://valtioneuvosto.fi/documents/10616/1986338/VNKJ092016+en.pdf/b33c3703-29f4-4cce-a910-b05e32b676b9

[6] Thiele R., "Crisis in Ukraine – the emergence of hybrid warfare", *ISPSW strategy series: focus on defense and international security* 347 (2015): 1

[7] Baun E., "The digital underworld: cyber crime and cyber warfare", *Humanicus* 7 (2012): 2

[8] World Economic Forum, *supra* note 3

[9] Baun E., *supra note* 6, 2

[10] BBVA Research, "Digitial Economy Outlook" (2016) // https://www.bbvaresearch.com/wp-content/uploads/2016/03/DEO_Mar16_Cap2.pdf

[11] Appazov A., "Legal aspects of cyber security" // http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

[12] Lewis A. James., "Assessing the risks of cyber terrorism, cyber war and other cyber threats" // https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

[13] Baun E., *supra note* 6, 2

[14] Solis D. Gary, The law of Armed Conflict. International Humanitarian Law in War (Cambridge University Press, 2016), 679

[15] Herzog S., "Revisiting the Estonian cyber attacks: digital threats and multinational responses", *Journal of strategic security* 2 (2011): 52

[16] Solis D. Gary., *supra note* 13, 679

[17] Baun E., *supra note* 6, 7

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

commerce[18]. Last but not the least, cyber operation launched in 2011 by hacktivist group Anonymous on Sony's Playstation Network caused approximately $170 million in losses for the company[19]. Pinnacle of an unprecedented deterioration of cyber security were 2015 cyber engineered attacks on Ukraine's power grid. As an aftermath of the severe blackout 700,000 households were affected[2021].

Ultimately 2016 world's largest DDoS attack amounting to 1Tbps disabled French internet service provider OVH. Whereas bearing in mind the fact that merely 1Gbps attack is sufficient to knock most businesses anywhere in the world offline[22].

Hence, cyber security concerns per se are relevant to public and private sectors. Ensuring security and integrity of data has become a challenging issue in terms of functioning of states and businesses entities which rely massively on digital communications and networks.

Increasing awareness on the part of the states and international community towards undertaking solid measures in the field of cyber space protection was essential, however a belated response. It served as a trigger for the adoption of a numerous cyber security strategies on the national level. Foreign, security and defense policies were underpinned by cyber domain[23]. Perception of national security through the component of cyber space developed into a prevailing one. To a great extent, as outlined in The National Strategy to secure Cyberspace of 2003, it was also deemed essential to the economy[24].

The United Kingdom's cyber security strategy of 2009 has a reflection of cyber risks: "just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space"[25]. In essence analogous statements were envisaged in the US approaches towards cyber threats, regarded as most serious economic and national security challenges of the 21st century for the US and its allies[26].

Emerging cyber security policymaking was also pushed by the expanding occurrences of business exposure to cyber risks and financial damages. Field surveys of 2017 provide manifestation of business being already in a disposition to strengthen security in the cyber space. Continuing security breaches to the detriment of the sustainable business development (for example, in consonance with the United Kingdom's Information Security Breaches Survey of 2014 almost 81% of large companies reported security breaches, costing each organization on

[18] Tully S., "Protecting Australian cyberspace: are our international lawyers ready?", *Australian International Law Journal* 4 (2012): 62

[19] Appazov A., *supra note* 10

[20] BBVA Research, *supra note* 9

[21] TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense (March 18, 2016) // https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[22] "ACS. Cybersecurity. Threats. Challenges. Opportunities", *supra note* 2

[23] Prime Minister's Office Publications. Government report on Finnish Foreign and security policy, *supra note* 4

[24] Executive Office of the President of the United States, "The National Strategy to Secure Cyberspace" (2003) // https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

[25] Cabinet office,"Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space", (June, 2009) // https://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

[26] US. National security Council and Homeland Security Council, "Assuring a trusted and resilient information and communications infrastructure", (2009) // https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

average between £600,000 and £1.5m.[27]; another piece of data demonstrates that cyberattacks are costing global businesses as much as $500 billion per year[28]) have resulted in visible adjustments. Prioritizing cyber security comprises 74 % of the UK businesses and 67 % of the UK businesses are investing money in favor of averting cyber threats.[29]

Accordingly, such a drastic shift in the global dimension occurred on account of several reasons.

Firstly, digital world is not contingent on the control of a single entity[30]. Decentralized environment of cyber space operating within loose regulation, in contrast to hierarchical composition of states, granted multiple actors unrestricted access to the diffused power[3132]. Decentralized cyber space, despite being the original intention, has paved way for today's vulnerable network[33].

Akin transformation of cyber space was targeted at undermining the exclusiveness of a state. Insecurity risks caused by the cyber threats erode conjointly public trust[34], and so impairing credibility of the state's institutions, undoubtedly also posing far-reaching effects.

Commonly cyber space is used as a tool for compromising states. By means of leveraging cyber operations other actors may achieve a number of tangible strategic goals. In this respect states and individuals, for example, possess same abilities to deliver harmful cyber effects[35]. Such actor pattern of rivals in the domain of cyber space shape asymmetry thereby empowering individuals[36].

Secondly, actions in the cyber space are scarcely subject to the constraints of sovereignty or jurisdiction[37] and respectively coining complexities for existing legal systems to deal with cyber threats. Contemporary cyber world is furtive[38]. Covert operations in the cyber space are carried out under high degree of anonymity, an obvious advantage for disguising perpetrators' identities[39], are favorable to creating situations which are ambiguous and blur from the standpoint of law. Usually in the present circumstances of perpetrators identity contestability political decisions are just pending[40].

---

[27] The Information security arm of GCHQ, "Common Cyber Attacks: reducing the impact" (2015) // https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

[28] "ACS. Cybersecurity. Threats. Challenges. Opportunities", *supra note* 2

[29] "Cyber security breaches survey" (2017) // https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

[30] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity strategy of the European Union: an open, safe and secure cyberspace" (2013) // http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[31] Appazov A., *supra note* 10

[32] Tully S., *supra note* 17, 71

[33] Baun E., *supra note* 6, 7

[34] Thiele R., *supra note* 5, 3

[35] Solis D. Gary., *supra note* 13, 685

[36] Appazov A., *supra note* 10

[37] Appazov A., *supra note* 10

[38] Baun E., *supra note* 6, 1-2

[39]Appazov A., *supra note* 10

[40] Rid T., Buchanan B. "Attributing cyber attacks", *The Journal of Strategic Studies* 38 (2015): 4

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

Foremost it refers to the difficulties connected with tracking perpetrators[41], likewise identifying offender's jurisdiction[42][43], thus framing risks of impunity. Yet another perplexing obstacle here relates to finding evidence[44], apt to quick destruction[45].

Akin actions might be confronted with legal restrictions. In substance the complicacies arise with the deficiency of international agreements of mutual assistance[46]. However even the legal framework itself should not be overestimated. Sophisticated nature of cyber threats presupposes corresponding methods of operations execution in the cyber domain (cyber attacks wired by an adversary through the territory of third states; remote computer hijacking for the purpose of a cyber-attack; coordinated cyber-attack from different locations).

Attribution of conduct[47] becomes overwhelmingly significant in light of either national, or international legislation, depending on the type of cyber threat employed against the adversary. The importance of establishing attribution also consists in the issue of distinguishing the offender between state or non-state actors[48] which would further have specific legal effects.

Establishing a link between a conduct in the cyber domain and the specific entities remains a vexing challenge. Subsequently an attribution of behavior, together with determination of the source, location and the identity of an attacker, is exceedingly critical for accountability enforcement. Traceability of the cyber threats is less problematic in case of military networks but quite complicated within the domain of civilian networks, like Internet[49].

The identification of perpetrator in terms of cyber activities is complicated by a number of reasons (both of technical and nontechnical by nature)[50]. In substance, it is profoundly dependent on the availability of evidence along with its accessibility.

Existing difficulties in the determination of attribution of conduct are also impeding framing of potential responses[51]: deterring cyber threat, starting legal proceedings, launching counterattack, imposing sanctions[52]. It is becoming peculiarly sensitive through the perspective of a cyber-attack, authorizing states to invoke self-defense (even the possibility of anticipatory or preemptive self-defense is not excluded either) as a justification for using force against adversary in a response to a cyber-attack[53].

Shortage of plausible evidence comfortably prompts appealing to indefinite auxiliary clues.

---

[41] *Ibid.*, 5

[42] Appazov A., *supra note* 10

[43]Tully S., *supra note* 17, 55

[44] Rid T., *supra note* 39, 6

[45] Appazov A., *supra note* 10

[46] Baun E., *supra note* 6, 21

[47] Solis D. Gary., *supra note* 13, 685

[48] Appazov A., *supra note* 10

[49] Rowe C. Neil "Deception in Defense of Computer Systems from Cyber Attack" // http://calhoun.nps.edu/bitstream/handle/10945/36424/Rowe_Deception_in_defense_of_computer.pdf?sequence=1

[50] Schreirer F., "On cyber warfare On Cyberwarfare" // http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf

[51] Ibid.

[52] Rowe C. Neil, *supra note 49*

[53] Dunlap J. Charles. Jr., "Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly* Spring (2011): 87

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

Some indicators (target, malware, motive and complexity), although to some degree bearing significance are still inconclusive[54]. Application of alike means, for example approaching attribution through the prism of beneficiary, are mostly misleading[55]. Also, the denial of attribution combined with refusal to cooperate with investigation of cyber incident might serve as an indication of guilt[56]. Nevertheless, the latter by nature are at large founded on conjectures being in this manner inadmissible from the standpoint of law.

For the sake of accurate cyber threat tracking it is necessary to validate that the attack originated from the specific source[57]. Even in case of successful localization of cyber threat does not suffice for the purposes of attribution. Present circumstance alone is still unsatisfactory in terms of providing undeniable proof for entity's complicity in cyber threat[58]. In fact, the computers exploited for the pernicious purposes might be operated remotely by third parties[59]. Namely, perpetrators empowered by false IP addresses, foreign serves and aliases enjoy anonymity and relative impunity[60], likewise inclined to claiming deniability. Moreover, it is noteworthy that evolving nature of cyber threats subject to permanent sophistication increasingly diminishes the chances of their uncovering[61].

Detection and disclosure of evidence in the cyber domain is another issue of concern. Difficulties are commonly stemming out of the architecture of digital environment. Its shortcomings basically refer to the deficiency of distinct physical evidence[62]. Besides the digital evidence, due to being ephemeral in nature and susceptible to manipulation, raises issues of its reliability[63]. Yet, the process of retrieval and retention of evidence from the digital systems is difficult and time consuming and still it requires cooperation from the digital infrastructure providers[64]. Whereas, conveniently deployable cyber threats are, in comparison to likely risks, extensively rewarding for cyber trespassers[6566].

Additionally, another confronting issue of advancing cyber security relates to state jurisdiction[67]. Forasmuch as cyber threats normally operate within the realm of interstate relations, the jurisdictional boundaries challenge them. In the event of investigation and law

[54] Geers K., "Cyber war in perspective: Russian aggression against Ukraine" // https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

[55] Libicki C. Martin, "Cyberdeterrence and cyberwar" // http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

[56] Ibid.

[57] Gunneriusson H., "Nothing Is Taken Serious Until It Gets Serious: countering hybrid threats", *Defence Against Terrorism Review* 4 (2012): 60

[58] Libicki C. Martin., *supra note* 55

[59] Singer P., Friedman A., "Cyber security and cyber war. What everybody need to know" // https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf

[60] Schreirer F., *supra note* 50

[61] Schreirer F., *supra note* 50

[62] Libicki C. Martin, *supra note 55*

[63] Schreirer F., *supra note* 50

[64] Cyber resilience: how to protect small firms in the digital economy // http://www.fsb.org.uk/docs/default-source/fsb-org-uk/FSB-Cyber-Resilience-report-2016.pdf?sfvrsn=0

[65] Ibid.

[66] Schreirer F., *supra note* 50

[67] Gunneriusson H., *supra note* 57, 60

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

enforcement due emphasis must be inevitably placed on jurisdiction[68]. Barriers of state jurisdiction impose restraints on the performance of such actions. In pursuance of overcoming jurisdictional constraints, it is appropriate to resort to concluding international agreements on mutual legal assistance[69] (encompassing issues of request execution, exchange of information, law enforcement, sanctions, extradition etc.[70]).

HYBRID THREATS

Regardless of its common usage, the hybrid threat is not an easily definable concept[71]. Elaboration of a meaningful broadly accepted "hybrid threat" definition is barely unattainable. Hybrid threats due to their highly evolving nature[72] currently remain beyond the scope of uniform conceptualization. Prevailing flexibility in the interpretation of hybrid threats incorporates equally advantages and shortcomings.

Hybrid threats are basically regarded as a blend of diverse types of military and non-military instruments utilized by state or non-state actors to compromise the adversary[73][74]. Amid existing myriad of hybrid threats cyber engineered threats represent a paramount hazard to the national security, state's political and economic integrity. Subtle nature of cyber threats exacerbates threat assessment process, especially identification and determination of cyber threats. Generally, unpredictability and sophistication emanating from hybrid threats complicates their timely disclosure. Indeed, victims of cyber operation become aware of it long after the event[75][76]. The identification of cyber threats, pursuant to the expertise research, may endure 416 days[77].

[68] Cybersecurity: The Role and Responsibilities of an Effective Regulator // http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf

[69] Dunlap J. Charles. Jr., *supra note 53,* 83

[70] The Growing Global Threat of Economic and Cyber Crime // http://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf

[71] Joint Communication to the European Parliament and the Council Joint Framework on Countering, "Hybrid Threats a European Union Response" (2016) // http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

[72] Lloyd's, "Emerging risk report", (2015) // https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/bitcoin--final.pdf

[73] Prime Minister's Office Publications. Government report on Finnish Foreign and security policy, *supra note* 4

[74] Bachmann S.-D. "Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management"*Amicus Curiae* 88 (2011):24

[75] Lloyd's, "Emerging risk report", *supra note* 49

[76] The Information security arm of GCHQ, *supra note* 26

[77] Wong A., Eng C., Yao R., Ng J. "Cyber threats in hybrid warfare: securing the cyber space for the RSAF" *Journal of Singapore Armed Forces* 1(2016):28

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

CRITICAL NATIONAL INFRASTRUCTURE AND LEGAL FRAMEWORK

Currently the preservation of *critical national infrastructure*[78] is a matter of meticulous consideration in terms of national security[79]. Ample dependence of states operational activities on the computer networks favors external intrusions by different actors for the sake of obtaining beneficial advantages. Cyber-attacks on the critical national infrastructure (power, water, traffic control, refinery, banking, finance systems etc.[8081]), however lacking any clear-cut content[82], varying from country to country[83], and thus being far from enjoying any uniform understanding, pertain to the gravest national security threats, capable of substantially dismantling states institutional capacity, generating economic damages, societal disruption and might even lead to casualties[848586]. In general mass web destruction, spam, malware infection, ransomware, spyware, social engineering, and even alterations to physical devices are indispensable components of cyber-attacks[8788].

Approaching cyber-attack from this standpoint gives rise to its distinction from other forms of activities in the cyber space (cyber-crime, cyber intrusions, cyber terrorism, cyber espionage, hacktivism and other related cyber operations[8990]). Disrupting IT infrastructure in order to affect decision making process typically falls under the definition of a cyber attack[91].

Tackling cyber-attack is a principally sensitive issue inasmuch meeting certain criteria (causing injury or deaths to persons, either damage, or destruction to objects[92]) it may constitute a use of force and as a consequence authorizes a state to act in self-defense, as proscribed by the pertinent provisions of the UN Charter (article 2(4), 51). Resort to a cyber-attack triggers the applicability of norms and principles of international law (Tallinn manual on the international

[78] Tully S., *supra note* 17, 50
[79] Lewis A. James, *supra note* 11
[80] Solis D. Gary., *supra note* 13, 679
[81]Tully S., *supra note* 17, 51
[82] Eckert S. "Protecting Critical Infrastructure: The Role of the Private Sector" // http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf
[83] Cybersecurity: The Role and Responsibilities of an Effective Regulator, *supra note 68*
[84] Appazov A., *supra note* 10
[85] Siboni G., Y.R. "What lies behind Chinese cyber warfare" *Military and Strategic Affairs* 2 (2012): 49
[86]Joint Communication to the European Parliament and the Council Joint Framework on Countering, supra note 48
[87] "ACS. Cybersecurity. Threats. Challenges. Opportunities", *supra note* 2
[88] Bachmann S.-D., *supra note* 51
[89]Tully S., *supra note* 17, 64
[90] Solis D. Gary., *supra note* 13, 674
[91] A M&S architecture and tools for security issues analysis countering hybrid cyber warfare threats // https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-143/MP-MSG-143-22.pdf
[92] Appazov A., *supra note* 10

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

law applicable to cyber warfare (2013)[93], Cyber security Strategy of the European Union (2013)[94], Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications (2015)[95].

In view of this, arbitrary usage of the term cyber attack to denote other types of threats in the cyber domain is not only unacceptable but also erroneous[96]. It is completely void of understanding cyber attack's nature and its distinctive features.

Whilst international legal framework for fostering cybersecurity was imperceptibly successful. Incentives undertaken display some degree of international organizations engagement in the promotion of cybersecurity. Few resolutions, adopted by the UN General Assembly, drew attention to the intricacies of the cyber security. Endeavors of the international community to reinforce protection of critical information infrastructures, as well as prevention of cyber-attacks were explicitly envisaged in two resolutions (A/Res/55/63 (2001)[97]; A/Res/58/199 (2004)[98]. Yet UN's involvement was also bestowed upon cyber-crime, expressly specified in a comprehensive study on cyber-crime, prepared in 2013 by UN office on drugs and crime[99]. Other actions advocating cyber-security, in conjunction with the above-mentioned soft law instruments, are implemented through UN institutional pattern, namely International Telecommunications Union – UN *specialized agency* for information and communication technologies; UN Economic Commission for Africa. In 2016 by virtue of backing regional cyber-security enhancement model cross-border laws (on telecommunications, cyber-security) were enacted by Central African States[100]. Still cyber-security as a part of global agenda is only evolving[101].

In contrast to UN, cyber-security challenges were addressed with due regard by international regional organizations and most notably on the national level. It is consonant with the engagement of EU, NATO, Council of Europe and some individual state initiatives. The EU has endorsed hitherto its cybersecurity strategy of 2013[102], instituted in 2016 Hybrid Fusion Cell as a

[93] Tallin Manual on International Law applicable to cyber warfare (2013) // https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

[94] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *supra note* 29

[95] UN, "Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications" (2015) // http://undocs.org/en/A/70/172

[96] On Cyberwarfare Fred Schreier, 10

[97] UN General Assembly "Combating the criminal misuse of information technologies" (2001) // https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

[98] UN General Assembly "Creation of global culture of cyber security and the protection of critical information infrastructures" (2004) // https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

[99] UNODC "Comprehensive study on cyber crime" (2013) // https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[100] UN Economic Commission for Africa // http://www.uneca.org/stories/cyber-security-central-african-states-adopt-model-cross-border-laws

[101] BBVA Research, *supra note* 9

[102] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *supra note* 29

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

framework on countering hybrid threats[103] and also provided for cross-institutional cooperation with NATO.

Compatible actions in the realm of cyber security were initiated by NATO: cooperative cyber defense center of excellence (2008)[104], cyber defense concept (2008), cyber defense pledge (2016)[105]. NATO also released a number of acute statements along with bolstering cyber security. The application of article 5 of the Washington Treaty in the event of cyber-attack was the outcome of NATO summit in Wales in 2014[106]. Unlike aforesaid, the provisions, for instance, of Security Treaty between Australia, New Zealand and the USA (ANZUS) (1951)[107] stipulate consultations between parties given cyber-attack[108]. And finally input by the Council of Europe embodies the Convention on Cybercrime (2001)[109] and action against cybercrime (2006)[110].

Substantial progress in advancing cyber-security is exemplified by unilateral actions of states on the domestic level. Various states tend to elaborate cyber security strategies, as well as consistently refine upon the existing strategies (USA Department of Defense Cyber Strategy (2015)[111]; Australia's cyber security strategy (2016)[112]; UK National Cyber Security Strategy 2016-2021[113]; Ukraine's Strategy of Cyber Security (2016)[114] etc.). Fortification of cyber security is still executed through the installation of appropriate mechanisms: Finland's Centre of Excellence for countering hybrid threats (2017) [115][116], Australia's Cyber Security Center (2013)[117], UK's National Cyber Security Center (2016), US Cyber Command (2010) and others.

---

[103] Joint Communication to the European Parliament and the Council Joint Framework on Countering, supra note 48

[104] NATO, "Cyber Defense Concept" (2008) // https://ccdcoe.org/history.html

[105] NATO, "Cyber Defense Pledge" (2016) // http://www.nato.int/cps/en/natohq/official_texts_133177.htm

[106] Understanding Hybrid Threats // http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf

[107] Security Treaty between Australia, New Zealand and the USA (1951) // http://australianpolitics.com/1951/09/01/anzus-treaty-text.html

[108] Tully S., *supra note* 17, 59

[109] Council of Europe, "Convention on Cybercrime" (2001)// https://rm.coe.int/1680081561

[110] Council of Europe, "Action against Cybercrime" (2006) // https://www.coe.int/en/web/cybercrime/home

[111] The Department of Defense, "Cyber Strategy" (2015) https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[112] Australian Government, "Cyber security Strategy" (2016) // https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

[113] HM Government, "National Cyber Security Strategy" (2016-2021) // https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[114] Стратегія кібербезпеки України (Ukraine's cyber strategy) (2016) // http://www.president.gov.ua/documents/962016-19836

[115] EU press release // https://eeas.europa.eu/headquarters/headquarters-homepage_en/24572/EU%20welcomes%20establishment%20of%20the%20Finnish%20Centre%20of%20Excellence%20for%20countering%20hybrid%20threats

[116] Prime Minister's Office Publications. Government report on Finnish Foreign and security policy, *supra note* 4

[117] "ACS. Cybersecurity. Threats. Challenges. Opportunities", *supra note* 2

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

Present developments in the sphere of countering cyber-crime are more rewarding in comparison to progress in safeguarding cyber-security universally and consecutively subverting the prospect of a comprehensive multilateral cyber security treaty.

Proliferation of cyber operations, aimed at the effective exploitation of vulnerabilities (occurring faster than defenders could remedy them[118]), prompted the endorsement of cyber resilience strategies.

A blueprint for cyber security agenda is a vulnerability reduction[119]. Today's predominant disposition to cyber security rests on a comprehensive (integrated) approach encompassing an array of instruments (military, non-military, intelligence operations and police investigations; information and social media campaigns etc.)[120][121]. Likewise some crisp ideas are put forward: a proactive stance in cyber security[122], cyber attack data sharing[123] which are backed by the other proposed options with the aim of strengthening cyber security, including some measures on the international and domestic level. For example, international cooperation[124], information sharing, interagency coordination [125], improvement of laws and regulations [126], public-private partnerships[127] etc. Despite the fact that the outcomes of such incentives are still unclear, but it is already obvious that multiple actors such as states, private entities and individuals should be the key players in pushing the cyber security issues. Participation of the latter is an essential prerequisite for the securing of cyber space.

The imperfection of its genuine efficiency call for the continuing search of alternatives. Artificial intelligence could be a worthwhile option to consider. Incorporation of artificial intelligence technologies into a cyber domain could present a promising solution to consolidating cyber security.

Noticeable advantages pertinent to the artificial intelligence relate to its vast capacities, especially in comparison to human beings, for shielding cyber security. Operating systems equipped with artificial intelligence expedite the large-scale detection of cyber threats, mitigate cyber risks and generally being less prone to errors. Furthermore, current efficiency of the artificial intelligence is subject to its further improvement.

The utilization of artificial intelligence in cyber security is ostensibly irresistible. Although by no means it should be viewed as a comprehensive remedy in this respect. By contrast, some restraints of the artificial intelligence essentially should be taken into account.

In terms of the latter, it represents a tool of dual nature being both suitable for the purpose of defense and attack. States aspirations to master the artificial intelligence with high probability

---

[118] Lloyd's, "Emerging risk report", *supra note* 49

[119] Common Cyber Attacks: reducing the impact, *supra note* 26

[120] Thiele R. *supra note* 5, 9

[121] Ratiu A., "Countering hybrid threats by integrating civilian-military capabilities". *International conference knowledge based organization.* 1 (2016):109-110

[122] Accenture, "Intelligent security: defending the digital business" (2016) // https://www.accenture.com/t20160722T052642__w__/us-en/_acnmedia/Accenture/Conversion-Assets/MainPages/Documents/Global/Accenture-Defending-Digital-Business.pdf

[123] Lloyd's, "Emerging risk report", *supra note* 49

[124] Cybersecurity: The Role and Responsibilities of an Effective Regulator, *supra note* 68

[125] The Department of Defence Cyber strategy, *supranote 111*

[126] The Growing Global Threat of Economic and Cyber Crime, *supra note* 70

[127] Cyber resilience: how to protect small firms in the digital economy, supra note 64

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

will generate the arms race. Besides some existing premonitions about the future of the artificial intelligence are already reasonably being put forward. The major uncertainty is connected with the impending risk of losing control over the artificial intelligence on account of rampant development of its scope.

Incorporation of artificial intelligence into cyber security systems at least requires combination of computers and humans, contributing to resilience to cyber threats.

CONCLUSIONS

Cyber domain is a hostile environment with abundant security risks, equally dangerous for states, businesses and individuals. Cyber threat converted it into a powerful weapon, an object of rivalry between numerous actors. Adversaries have not exhaustively disclosed the capacity of cyber threats, and hence such an obscurity is even more dangerous than ever. We need to be alert. Individuals and businesses perpetually are standbys in the process of cyber security, whilst frequently victimized by cyber threats. In the advent of smart cities, massively accessible autonomous cars and other digitally operated systems it is due time to consider about our active engagement in contributing cyber security. Imminent acknowledgement of a comprehensive model of cyber security as a response to the exigencies of cyber threats means its indivisibility for states, international organizations, society, businesses, entities, and human beings.

BIBLIOGRAPHY

1. A M&S architecture and tools for security issues analysis countering hybrid cyber warfare threats // https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-143/MP-MSG-143-22.pdf
2. Accenture, "Intelligent security: defending the digital business" (2016) // https://www.accenture.com/t20160722T052642__w__/us-en/_acnmedia/Accenture/Conversion-Assets/MainPages/Documents/Global/Accenture-Defending-Digital-Business.pdf
3. "ACS. Cybersecurity. Threats. Challenges. Opportunities" (November, 2016) // https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf
4. Appazov A., "Legal aspects of cyber security" // http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf
5. Australian Government, "Cyber security Strategy" (2016) // https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
6. Bachmann S.-D. "Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management"*Amicus Curiae* 88 (2011): 24-27
7. Baun E., "The digital underworld: cyber crime and cyber warfare", *Humanicus* 7 (2012): 1-25
8. BBVA Research, "Digitial Economy Outlook" (2016) // https://www.bbvaresearch.com/wp-content/uploads/2016/03/DEO_Mar16_Cap2.pdf

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

9. Cabinet office,"Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space", (June, 2009) // https://www.official-documents.gov.uk/document/cm76/7642/7642.pdf
10. Council of Europe, "Action against Cybercrime" (2006) // https://www.coe.int/en/web/cybercrime/home
11. Council of Europe, "Convention on Cybercrime" (2001)// https://rm.coe.int/1680081561
12. Cyber resilience: how to protect small firms in the digital economy // http://www.fsb.org.uk/docs/default-source/fsb-org-uk/FSB-Cyber-Resilience-report-2016.pdf?sfvrsn=0
13. Cybersecurity: The Role and Responsibilities of an Effective Regulator // http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf
14. "Cyber security breaches survey" (2017) // https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017
15. Стратегія кібербезпеки України (Ukraine's cyber strategy) (2016) // http://www.president.gov.ua/documents/962016-19836
16. Dunlap Charles J. Jr.," Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly* Spring (2011): 81-99
17. Eckert S. "Protecting Critical Infrastructure: The Role of the Private Sector" // http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf
18. EU press release // https://eeas.europa.eu/headquarters/headquarters-homepage_en/24572/EU%20welcomes%20establishment%20of%20the%20Finnish%20Centre%20of%20Excellence%20for%20countering%20hybrid%20threats
19. Executive Office of the President of the United States, "The National Strategy to Secure Cyberspace" (2003) // https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
20. Geers K., "Cyber war in perspective: Russian aggression against Ukraine" //https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf
21. Gunneriusson H., "Nothing Is Taken Serious Until It Gets Serious: countering hybrid threats", *Defence Against Terrorism Review* 4 (2012): 47-71
22. Herzog S., "Revisiting the Estonian cyber attacks: digital threats and multinational responses", *Journal of strategic security* 2 (2011): 49-60
23. HM Government, "National Cyber Security Strategy" (2016-2021) // https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
24. "Internet World Stats. Usage and Population Statistics" // http://www.internetworldstats.com/stats.htm
25. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity strategy of the European Union: an open, safe and secure cyberspace" (2013) // http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
26. Joint Communication to the European Parliament and the Council Joint Framework on Countering, "Hybrid Threats a European Union Response" (2016) // http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

27. Lewis A. James., "Assessing the risks of cyber terrorism, cyber war and other cyber threats" // https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
28. Libicki C. Martin, "Cyberdeterrence and cyberwar" // http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
29. Lloyd's, "Emerging risk report", (2015) // https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/bitcoin--final.pdf
30. NATO, "Cyber Defense Concept" (2008) // https://ccdcoe.org/history.html
31. NATO, "Cyber Defense Pledge" (2016) // http://www.nato.int/cps/en/natohq/official_texts_133177.htm
32. Prime Minister's Office Publications. Government report on Finnish Foreign and security policy. (9/2016) // http://valtioneuvosto.fi/documents/10616/1986338/VNKJ092016+en.pdf/b33c3703-29f4-4cce-a910-b05e32b676b9
33. Ratiu A. "Countering hybrid threats by integrating civilian-military capabilities". *International conference knowledge based organization*. 1(2016): 109-114
34. Rid T., Buchanan B. "Attributing cyber attacks", *The Journal of Strategic Studies* 38 (2015): 4-37
35. Rowe C. Neil "Deception in Defense of Computer Systems from Cyber Attack" // http://calhoun.nps.edu/bitstream/handle/10945/36424/Rowe_Deception_in_defense_of_computer.pdf?sequence=1
36. Schreirer F., "On cyber warfare On Cyberwarfare" // http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf
37. Security Treaty between Australia, New Zealand and the USA (1951) // http://australianpolitics.com/1951/09/01/anzus-treaty-text.html
38. Siboni G., Y.R. "What lies behind Chinese cyber warfare" *Military and Strategic Affairs* 2 (2012): 49-64
39. Singer P., Friedman A., "Cyber security and cyber war. What everybody need to know" // https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf
40. Solis D. Gary, *The law of Armed Conflict. International Humanitarian Law in War*. Cambridge University Press, 2016.
41. Tallin Manual on International Law applicable to cyber warfare (2013) // https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf
42. The Department of Defense, "Cyber Strategy" (2015) https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
43. The Growing Global Threat of Economic and Cyber Crime // http://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf
44. The Information security arm of GCHQ, "Common Cyber Attacks: reducing the impact" (2015) // https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf
45. Thiele R., "Crisis in Ukraine – the emergence of hybrid warfare", *ISPSW strategy series: focus on defense and international security* 347 (2015): 1-13
46. TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense (March 18, 2016) // https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

47. Tully S., "Protecting Australian cyberspace: are our international lawyers ready?", *Australian International Law Journal* 4 (2012): 49-77
48. Understanding Hybrid Threats // http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf
49. UN General Assembly "Combating the criminal misuse of information technologies" (2001) // https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
50. UN General Assembly "Creation of global culture of cyber security and the protection of critical information infrastructures" (2004) // https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf
51. UN Economic Commission for Africa // http://www.uneca.org/stories/cyber-security-central-african-states-adopt-model-cross-border-laws
52. UN, "Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications" (2015) // http://undocs.org/en/A/70/172
53. UNODC "Comprehensive study on cyber crime" (2013) // https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
54. US. National security Council and Homeland Security Council, "Assuring a trusted and resilient information and communications infrastructure", (2009) // https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf
55. Wong A., Eng C., Yao R., Ng J. "Cyber threats in hybrid warfare: securing the cyber space for the RSAF" *Journal of Singapore Armed Forces* 1(2016):25-38
56. World Economic Forum. "The Global Risks Report" (12th edition, 2017) // http://www3.weforum.org/docs/GRR17_Report_web.pdf

SANTRAUKA

Šis straipsnis tarpdisciplininiškai (teisė (nacionalinė ir tarptautinė), politika, ekonomika bei filosofija) nagrinėja kibernetinės grėsmės problemą globalios verslo aplinkos srityje. Straipsnis susideda iš keturių dalių. Įžangoje pateikiami faktai, atskleidžiantys kibernetinės grėsmės autentiškumą ir didelio masto žalą, kurią patiria globalaus verslo organizacijos. Pabrėžiama, kad dabartinis kibernetinio domeno pažeidžiamumas yra decentralizuotos struktūros ir teisinio reguliavimo trūkumo pasekmė.

Antrojoje straipsnio dalyje dalyje kibernetinės atakos analizuojamos kaip mišrių grėsmių (ang. hybrid threats), kurios kelia pavojų šalių pagrindinėms funkcijoms, rūšis. Kibernetinės atakos, nukreiptos prieš šalių ypatingos svarbos infrastruktūras, pradėjimas gali lemti vienašalį arba bendrą savigynos, vadovaujantis tarptautine teise, taikymą. Dabartinis šiuolaikinės tarptautinės teisės taikymas kibernetinio saugumo srityje ženkliai sumažina naujo teisinio režimo pasirodymo galimybes.

Trečioje straipsnio dalyje „dėmesys sutelkiamas apibrėžiant ypatingos svarbos nacionalinės infrastruktūros sąvoką ir atitinkamai jos ryšį su kibernetinėmis grėsmėmis. Nepaisant fakto, kad ypatingos svarbos nacionalinės infrastruktūros sąvoka neturi vieningo

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No.2 (16), 2017, p. 17-33

apibrėžimo, šio apibrėžimo nustatymas priklauso šalių kompetencijai, priimant nacionalinius teisės aktus.

Autorius pabrėžia, kad kibernetinėje erdvėje priešininkai pritaiko daugelį sudėtingų rūšių operacijų, iš anksto numatančių skirtingus teisinius reguliavimus ir skirtingus atsparumo mechanizmus. Kibernetinė ataka, kuri yra didžiausia kibernetinė grėsmė, gali net iššaukti savigynos teisės panaudojimą. Šiais laikais jėgos panaudojimas negali būti suvokiamas klasikine, bet gana apribojančia prasme, turint galvoje tik kinetines priemones. Kibernetinės atakos yra naujos kategorijos jėgos, naudojamos tarptautiniuose santykiuose, pavyzdys. Greita skaitmeninės aplinkos plėtra iš esmės palieka užnugaryje jau egzistuojantį teisinį reguliavimą. Kibernetinės grėsmės yra susijusios su kibernetiniu saugumu universaliu (JT), regioniniu (ES, NATO) ir nacionalinio lygmeniu. Pažymima, kad užtikrinant kibernetinį saugumą turi būti įtrauktos irdirbtinio intelekto technologijos.

Vieningo, visiems tinkamo, požiūrio į kibernetinį saugumą trūkumas lemia poreikį ieškoti alternatyvų kibernetinio saugumo stiprinimui. Greta kitų pasirinkimų yra svarstytinas dirbtinio intelekto panaudojimas kibernetinėje srityje. Kadangi šalia akivaizdžių dirbtinio intelekto privalumų dažniausiai yra ir daug rizikos, nediskutuotina nauda, kurią teikia dirbtinio intelekto panaudojimas kibernetinio saugumo srityje, turi būti įvertinta kartu su šia rizika. Pastaroji daugiausiai susijusi su galimu dirbtinio intelekto pavirtimu ginklu, turinčiu antgamtinių bruožų. Daug žadančiai dirbtinio intelekto ateičiai (vadovavimas sudėtingoms sistemoms suderintas su daugiaprocesiniu režimu; kaip ir priešingas jo panaudojimas, siekiant pakenkti kitoms šalims), nors ir nesuvokiamai visa apimtimi, yra sunku atsispirti. Taigi, gali būti sovokiama kaip tiesianti kelią tolimesnėms ginklavimosi lenktynėms tarp šalių. Todėl pagrindiniai pokyčiai kibernetinio saugumo srityje bus įtakoti dirbtinio intelekto sistemų daugėjimo ir tolimesnio šių sistemų tobulinimo.

Apibendrinant straipsnyje pateikto tyrimo rezultatus, daroma išvada, kad priešininkams išsamiai neatskleidus kibernetinių grėsmių pajėgumų, tokia nežinia yra dar pavojingesnė nei kada nors anksčiau.

REIKŠMINIAI ŽODŽIAI

Anonimiškumas, atsakingumas, dirbtinis intelektas, elgesio priskirtinumas, globalizacija, internetas, jėgos panaudojimas, jurisdikcija, kenkimo programinė įranga, kibernetinės atakos, kibernetinis įsibrovimas, kibernetinės operacijos, kibernetinio saugumo strategija, kibernetinis domenas, mišrios grėsmės, nacionalinė teisė, rizikos įvertinimas, saugumo pažeidžiamumas, skaitmeninė aplinka, tarptautinė teisė.