IRSTI 10.87.85

Zh.I. Ibragimov[1], T.S. Assanova[2]

[1]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[2]Astana IT University, Astana, Kazakhstan
(E-mail: zhamaladen@mail.ru, t.assanova@astanait.edu.kz*)*

International law and its response to modern security threats that stem from developments in weaponry and technology

Abstract. *The emergence of new technologies such as nanoteachnology, cybertechnology, outer space and unmanned systems and its rapid development have had an impact on the existing rules of international law, and vice versa, due to advances in technology of weaponry. Handling such situations by law goes through interpretation by the 'old' international law and application to a new situation, or if necessary via the enactment of new law. In some cases, existing international law might be applicable to it by the extension of as the appropriate reinterpretation of international conventional norms as customary international law counterparts. Despite the fact that some international laws have been adopted during times of reduced development of technologies and weaponry types, they are nevertheless still likely to be applicable to the challenges and issues of security threats. Given the examples of using chemical weapons and cyber-attacks, this can be considered evidence of weaknesses of some international law norms due to interpretation issues as necessity to strength existing law through application of customary international law rules. Therefore, it is difficult to state that international law is unable to secure peace or help to avoid the threats inherent to new technology and weapons development because of states practice and the contribution of academics.*
Keywords: *International law, weaponry, technology, cyber-attacks, use of force, international customary law.*

DOI: https://doi.org/10.32523/2616-6844-2023-143-2-182-190

Introduction

The modern relationship between international law and weaponry through the employment of technology has been formalised in multilateral conventions on weapon varieties evolving from the 1868 St. Petersburg Declaration, which regulates the use of explosive projectiles to the 1899 Hague Declarations II and III, as concerning on the use of asphyxiating gases and the use of bullets, respectively [1]. However, the emergence of new technologies such nanoteachnology, cybertechnology, outer space and unmanned systems and their rapid development have had an impact on the existing rules of international law, and vice versa, due to advances in technology of weaponry. Handling such situations by law goes through interpretation by the 'old' international law and application to a new situation, or if necessary via the enactment of new law. In some cases, existing international law might be applicable to it by the extension of as the appropriate reinterpretation of international conventional norms as customary international law counterparts. However, in other situations 'the law has struggled to keep pace with technology' [2] due to a lack of multilateral treaty regulations. While cyber-attacks and use chemical weapons have had an impact on the development of technology through the modification of conflicts on the one hand, whilst inflaming controversy through the use and interpretation of international law on the other. Despite the fact that some international laws have been adopted during

times of reduced development of technologies and weaponry types, they are nevertheless still likely to be applicable to the challenges and issues of security threats. This paper will concentrate on two types of weaponry due to its proliferation. Firstly, development of technology will be analysed in relation to international law; then, chemical weapons and their associated controversy will be discussed. Finally, cyber-attacks in international relations and state responsibilities in this complex area will be examined.

Methodology

In this article, general scientific and special methods of legal science are applied. Thus, the method of analysis and synthesis, as well as the logical method, were used to form a holistic view of the development of technology and international law. The historical method applied to study the history of the formation of international law in the field of the weaponry. The empirical base of the research involved studying international treaties and cases of cyber-attacks occurred over the last decades.

Discussion

Technology development and international law: proportionality and discrimination. Although the development of high technology has advanced the quality of human life, it often is used in the evaluation of weaponry and certainly influenced on security threat through the military and defence situations as well in armed conflict. However, the contrary might also be true; for example, the latter is required and has stimulated technology enhancement due to necessity to address new methods of warfare. Moreover, the purposes of new technologies that have both civilian and military usage are referred to as 'dual-use' technologies [1]. Therefore, from the beginning on crystalizing of customary principles of superfluous injury or unnecessary suffering and indiscriminate attack, the enhancement of technologies hand-by-hand with weapons evolution raises requirements for flexibility of law to solve unexpected challenges. Nevertheless, technology is issued to clarify conventional provisions by providing the appropriate legal framework in more detailed and precise form, as, for example, in the Chemical Weapons Convention (CWC) with its Annex of detailed technological arrangements and provision clauses [3].

However, weapons using new technologies are likely to result in disproportionate and indiscriminate damage, which is banned by the general rules of the law of armed conflict, as well as customary international law [4]. One example is non-lethal weapons that employ new technology in relation to indiscriminate use could give rise to certain issues [5], as well as cyber-attacks where the destruction of computer programs through the use of a virus could affect untargeted computers. Both types of weapon could rapidly lead to grave consequences despite the minimum effort needed for their deployment.

Use of chemical weapons: the «types and quantities» for law enforcement purposes. The enactment of the CWC in 1993 was the one the great achievements of international multilateral treaty law, though the general movement towards the prohibition of these weapons that started in the mid-twentieth century. Moreover, when it entered into force it was supplemented by the creation of the organisational structure of Organisation for the Prohibition of Chemical Weapons [6]. Art. II(9) of the CWC lists purposes that are not prohibited under this convention; amongst these, one of the more debatable omission is the use of them for law enforcement, including for domestic riot control purposes. The definition of 'chemical weapons' in Art.II(1)(a) of the CWC states that 'Toxic chemicals and their precursors, … are not prohibited …, as long as *the types and quantities* are consistent with such purposes …' (emphasis added) [7]. Observing these two provisions appears to be controversial in reality. One particular example, for instance, could be the Chechen terrorist attack in a Moscow theatre in October 2002, when about 830 hostages were taken. Because of the use of the opiate fentanyl, an incapacitating chemical, by Russian security before the storming the theatre, about 130 hostages died. As a result, debates as to the controversy of the provisions and the use incapacitating chemicals for domestic riot control purposes have arisen, as a non-lethal weapons issue. While some scholars think that as such use, in combination with

conventional weapons, was necessary to save lives, others argue about the issues of distinction [5]. Both sides' concerns refer to the violation of the principles of international law in terms of international humanitarian law and international human rights. Moreover, questions about the CWC provisions regarding incapacitating chemicals and their use for law enforcement have arisen [8].

However, the principle concern is treaty interpretation where the relationship between the «types and quantities» for law enforcement requires careful examination. Dando claims that the concentration of chemical in part of a building, the effects on people as well as differentiating of lethal or incapacitating effects, and discrimination of individual's unconsciousness or breathing is most challenging to control [9]. Although this particular example from Russia appears to be quite extreme, and with use of incapacitating chemicals being otherwise legitimate [9], this incident nevertheless contradicted the state's obligation to protect the right to life with no derogation from this right for any reason, including an emergency [10].

Therefore, the «types and quantities» rule interpretation should consider international human rights law as being most relevant. Moreover, in this context the «types and quantities» rule in a law enforcement situation, the scope for the use of incapacitating chemicals is itself limited by the scope of international human rights law in this regard. The reality of using of chemical weapons and incapacitating chemicals shows that the CWC does not provide any clear definition of terms such as «law enforcement» or «types and quantities». Therefore, treaty interpretation practice is required [8].

Cyber-attacks as a new type of threat or use of force. Due to the development of technology and increasingly sophisticated computer programs, cyber-attacks are not only a new technology, also it used in a battlefield between the States and non-state actors. For instance, a cyber-attack with serious consequences was launched on 27th April, 2007, via a DDoS (distributed denial of service) attack that shut down the Estonian government and other private sector websites for a two-week period; it stopped the usual activities of the banking system, government services, and telecommunications. As this incident occurred at the same time that signs of the previous Soviet period were being removed, such as the «Bronze Soldier of Tallinn» monument to World War II which was alter called the «Bronze Soldier Attack». The DDoS method was found as the less adverse type of cyber-attacks which is used among the States with volume and size of this kind of incidents is not such a large-scale, although it would be grave and negative in comparison with this case. Given the capacity a cyber incident of this scale would require implied the connection to a state (probably Russia, or from its territory, in this instance). Although the cyber-attacks were directed from various places worldwide, the beginning and end of these distributed attacks were simultaneous [11].

This incident was the object of major international condemnation and academic debate as to whether it constituted a threat or the use of force against Estonia under Art.2(4) of the UN Charter. It is worth noting that this norm is a cornerstone of international law and states that 'all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, …' [12]. Reflection of this provision to customary international law and to peremptory norms of *jus cogens* was supported by the International Court of Justice (ICJ) in its case reports of Nicaragua v. US [13, paras 187-190] and Legal consequences of the construction of the wall in the occupied Palestinian territory [14, para 87].

'Art.2(4)'s express prohibition is both straightforward and ambiguous' [15, 427], and therefore it allows considerable latitude as to the interpretation of its meaning and usage. Some scholars argue that the cyber-attack in Estonia did not have particularly severe consequences, and therefore did not violate the norms of Art.2(4), even though bank and communication systems were targeted as critical infrastructure [16]. It is important to note the arguments of a number of scholars regarding the necessity of meeting the conditions of Art.2(4) and the application of customary law rules as regards cyber-attack. Roscini gives three main reasons for it: first, attribution of the cyber operation to states only,

because other subjects of international law do not fall under the scope these provisions. Another reason is the existence of a 'threat' or the 'use of force', and, finally, these actions must be conducted in 'international relations' [16]. Furthermore, Green argued that in majority view cyber-attacks that do not result in any physical damage or destruction do not fall within the scope of Art.2(4), and are more analogous to economic force [17].

Scholars have debated the interpretation of the words 'use of force' since the 1970s. Some argue that it depends on how much harm it causes. While some scholars argue that economical pressure does not constitute the use of force, others claim that cyber-attacks could fall under of the definition of use of force, just with a difference level of adverse effects. Consequently, the question arises as to what the threshold that one might consider a 'use of force' actually is. Roscini states that cyber-attacks that result in material damage of property, or injury or loss of life, as well as severe disruption of critical infrastructure functions are considered to constitute a 'use of force' under Art.2(4) and are thus prohibited by customary international law [16]. Similarly, Dinniss states that if cyber-attacks, in their various forms, either directly or indirectly cause the physical destruction of property, injury or loss of life, then they will fall under the scope of Art.2(4) as the 'use of force'. However, author goes on to claim that minimal physical consequences, or their absence, does not constitute the use of force, and therefore does not fall within the scope of Art.2(4). Nevertheless, this does not mean that such attacks are permitted. Moreover, as an illegal interference with a state's affairs, such an attack might be seen as a threat to peace and security. [18] Although the consequences and effects of cyber-attacks are not necessarily serious, or if they do not target critical infrastructure, it is unlikely that it can be claimed that they are somehow lawful purely because they do not violate Art.2(4). However, it is interconnected with principle of non-intervention [19].

Debates as to the applicability of existing norms of international law to threats from new types of technology and weapons such as cyber-attacks, and the absence of multilateral treaty in this area, have certainly lead to various types of interpretation and perspectives in this regard. Attempts to adopt multilateral treaties on information security were initiated by Russia, for instance [20], which prepared a draft Convention on International Information Security, that was subsequently released at an international meeting in Yekaterinburg in September 2011 [21]. Despite the absence of any multilateral treaties regulating this type of technology and weaponry and their obvious necessity, any attempts to produce such treaties appear thus far to have been unsuccessful. Although some scholars argue as to the applicability of 'old' law to cyber operations, though it is challenging, such a multilateral treaty would clarify area of use cyber operations as a valuable guidance [17]. Nonetheless, Waxman claims that efforts towards treaty regulation, particularly regarding cyber operations in comparison to Charter law would be less effortable. Charter law has the advantage of shaping state practice irrespective of the consent, or otherwise, of international actors, contrary to the adoption of a new treaty [15].

Are cyber-attacks weapons? If cyber-attacks can be considered the use of armed force, then it might be referred to the tool which is used as weapon [16] and general meaning of 'armed' connects with the equipping and using the weapon [22]. This leads to the necessity of defining what a weapon may actually be considered to be. Although the terminology of 'weaponry' is widely used within various legal frameworks, there is no binding definition of weaponry in international law within the *jus ad bellum* or *jus in bello* [16]. Scholars refer to various law dictionaries in their attempts to determine the meaning of 'weapon'; for instance, Black's Law Dictionary provides the definition of a weapon as 'an instrument used in fighting' [22]. Another definition provided by the ICRC Study on Customary International Humanitarian Law is that of 'to commit acts of violence against human or material enemy forces' [4]. The HPCR Manual in Rule 1 (ff) defines a 'weapon' as 'a means of warfare used in combat operations, … causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects' [23]. In other words, a weapon is an instrument of force that has the effects and consequences of

causing damage or destruction. Moreover, the Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons of the ICJ states that the use of force in the Art. 2(4) of the UN Charter 'do[es] not refer to specific weapons. They apply to any use of force, regardless of the weapon employed' [24, para 39].

Results

State responsibility towards cyber-attacks or due diligence. State responsibility and attribution of cyber-attacks appears to be interconnected because a state is responsible for operations originating from its territory regardless of whether it is unable or unwilling to deal with them, or is unaware of such operations within its territory, even if perpetrated by non-state actors or individuals. Such issues are not only an issue for vast states, however, as they might also be challenging for small states with less capacity or ability to control their cyberspace. The ILC Draft Articles on State Responsibility provides for provisions of state responsibility in Art.8 if such individuals are '… acting on the instructions of, or under the direction or control of, that State …' [25]. However, Margules argues as to accurate accountability of the Draft Articles in to relation to the law with its connection to 9/11 attacks. Scholar goes further, stating that a state being held responsible for any cyber operation with its territorial jurisdiction is also excessive [2]. It might be true for some larger states, such as the United States, Russia and China, however, that there is less doubt of their capacity to control and their interest in such 'cyber-powerful' entities.

Some scholars claim the necessity to consider the state responsibility to due diligence. In light of the above issues of the applicability of the existing norms of international law, Green argues for seeking an alternative approach to solve this issue. He went on to state that other norms of international law are disregarded, such as the duty of due diligence, which could come over of issues in relation to Art.2(4) [26]. Rule 6 of the Tallinn Manual 2.0 provides that '[a] State must exercise due diligence in not allowing its territory, … or cyber infrastructure … to be used for cyber operations that … produce serious adverse consequences for, other States' [19]. However, it provides this as a general principle, rather than a duty, or obligation or responsibility, and certainly not as the duty to prevention either. It is stated that the application of this principle is not used in a cyber operation context because it has not yet achieved the level of *lex lata* [19]. Nonetheless, this manual is not binding, though it is likely to be considered an authoritative guide for states practice.

The ICJ *Corfu Channel* case refers to the definition of the duty of due diligence as being 'every State's obligation not to knowingly allow its territory to be used for acts contrary to the rights of other States' [27]. Therefore, the state sovereignty principle forms a basis for the due diligence principle, because a state should take all necessary measures within its sovereign prerogatives. However, the state is not obligated to seek outside assistance in this regard, in the view of experts [19]. But it seems not a full due diligence if State would not to seek all reasonable measures of not causing harm to another State, especially when State is not economically developed. It appears to be challenging to justify State's not violation of due diligence principle then.

Some scholars claim about likelihood of advantageous consequences applicability of due diligence to cyber operations because States would be responsible for taking all necessary measures to prevent acts of cyber-attacks originating from the their territory [16]. However, others gave misinterpretation of this approach as connecting responsibility for cyber-attacks to that State particularly [28]. Although application of this general principle of due diligence to cyber-attacks is not often used in practice, it is likely to be supported by states practice as similarly States' preventive actions in international terrorist attacks and environmental issues [26].

Conclusion

In conclusion, it is important to note that the capacity of international law to secure peace and avoid threat goes together with the interpretation of treaty law, as well as customary international law, through states practice in order to respond to the threats posed by technology and weapons. Although some international rules were adopted many

years ago when technology and weaponry were relatively modest, and further that there is a current lack of multilateral treaties regulating specific issues – cyber-attacks, for instance – scholars nevertheless claim the applicability of 'old' international law to these modern concerns. Moreover, they argue that the flexibility that of these rules, as well as customary international law, can still be used extensively [16]. Given the examples of using chemical weapons and cyber-attacks, this can be considered evidence of weaknesses of some international law norms due to issues of interpretation issues as necessity to strength existing law through application of customary international law rules. Therefore, it is difficult to state that international law is unable to secure peace or help to avoid the threats inherent to new technology and weapons development because of states practice and the contribution of academics. Revisiting areas of existing customary rules such that of due diligence in the case of cyber-attacks could push to the margin the military side of using some norms such as use of force as being it only extremely needed cases [27]. Use of customary international law rules, therefore, create a basis for the application of international law rules to the unpredictable security threats arising from weaponry and technology development, in particular through addressing the gaps in treaty law and in its interpretation.

References

1. McLaughlin R., Nasu N. Introduction: Conundrum of New Technologies in the Law of Armed Conflict // New Technologies and the Law of Armed Conflict. – Asser Press, 2014. – P.1-20.

2. Margules P., Sovereignty and cyber-attacks: technology's challenge to the law of state responsibility // Melbourne Journal of International Law. – 2013. – Vol. 14. – P. 496-519.

3. Boothby, W.H. Weapons and the law of armed conflict. – Oxford University Press, 2nd edn, 2016. – 464 p.

4. Henckaerts, J-M., Doswald-Beck, L. Customary international humanitarian law, ICRC. – Cambridge University Press, 2005. – 689 p.

5. Coleman S. Ethical challenges of new military technologies in Nasu, N., McLaughlin, R. (eds) // New Technologies and the Law of Armed Conflict. – Asser Press, 2014. – P. 29-42.

6. Joyner, D.H. International law and the proliferation of weapons of mass destruction. – Oxford University Press, 2012. – 402 p.

7. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC), 13 January 1993.

8. Fidler D.P. The meaning of Moscow: «non-lethal» weapons and international law in the early 21st century // International Review of the Red Cross. – 2005. – Vol. 87(859). – P. 525-552.

9. Dando M. The danger to the chemical weapons convention from incapacitating chemical. First CWC Review Conference Paper. No. 4, University of Bradford, 2003. – 252 p.

10. Universal Declaration of Human Rights, Article 3, GA Res 217A (III), UN Doc. A/810, 1948; International Covenant on Civil and Political Rights, Articles 4 and 6, 19 December 1966, UNTS, Vol.999.

11. Valeriano, B., Maness, R.C., Cyber war versus cyber realities. cyber conflict in the international system. – Oxford University Press, 2015. – 288 p.

12. Charter of the United Nations, 26 June 1945.

13. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US), Merits, Judgment, 27 June 1986, ICJ Reports 1986.

14. Legal consequences of the construction of wall in the occupied Palestinian territory, Advisory Opinion, 9 July 2004, ICJ Reports 2005.

15. Waxman M.C. Cyber-attacks and the use of force: back to the future of Article 2(4) // The Yale Journal of International Law. – 2011. – Vol. 36. – P. 421-457.

16. Roscini, M. Cyber operations and the use of force in international law. – Oxford University Press, 2016. – 336 p.

17. Green, J.A. (Ed.). The regulation of cyber warfare under the jus ad bellum // Cyber Warfare. A Multidisciplinary Analysis. – Routledge Taylor & Francis Group, 2015. – P. 1-6

18. Dinniss, H.H. Cyber Warfare and the Laws of War. – Cambridge University Press, 2012. – 353 p.

19. Schmitt, M.N. (gen. ed.) Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. – Cambrdige University Press, 2017. – 302 p.

20. UN GA Doc. 'Role of science and technology in the context of security, disarmament and other related fields', A/53/576, November 18, 1998.

21. Russia's «Draft Convention on International Information Security» (2012). A Commentary. http://www.conflictstudies.org.uk/files/20120426_csrc_iisi_ commentary.pdf (accessed 15.12.2022).

Black's Law Dictionary, http://thelawdictionary.org (accessed 01.12.2022).

23. HPCR, Manual on International Law Applicable to Air and Missile Warfare, http://www.ihlresearch.org/amw/manual/section-a-definitions/weapon (accessed 20.12.2022).

24. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, ICJ Reports.

25. The ILC Draft Article on Responsibility of States on Internationally Wrongful Acts, 2001.

26. Green, J.A. Disasters Caused in Cyberspace in Breau, S.C., Samuel, K.L.H. (eds), Research Handbook on Disasters and International Law. – Edward Elgar Publishing, 2016. – P. 406-427.

27. Corfu Channel case (UK v Alb.), 1949 ICJ 4 (9 April).

28. Graham, D.E. (2010). Cyber threats and the law of war // National Security Law and Policy. – 2010. – Vol. 4. – P.87-102.

Ж.И. Ибрагимов[1], Т.С. Асанова[2]

[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

[2]Astana IT University, Астана, Қазақстан

Халықаралық құқық және оның қару-жарақ пен технологияларды дамытуға байланысты қауіпсіздіктің қазіргі қауіптеріне әрекеті

Аңдатпа. Нанотехнологиялар, кибертехнологиялар, ғарыштық және ұшқышсыз жүйелер сияқты жаңа технологиялардың пайда болуы және олардың қарқынды дамуы қару-жарақ технологиясының жетістіктері арқылы халықаралық құқықтың қолданыстағы нормаларына және керісінше әсер етті. Мұндай жағдайларды құқықтық реттеу «ескі» халықаралық құқықты түсіндіру және жаңа жағдайға қолдану немесе қажет болған жағдайда жаңа құқық енгізу арқылы жүзеге асады. Кейбір жағдайларда қолданыстағы халықаралық құқық оған қажет болған жағдайда халықаралық әдеттегі құқықтың аналогтары ретінде халықаралық конвенциялық ережелердің жаңа түсіндірмесін кеңейту арқылы қолданылуы мүмкін. Кейбір халықаралық шарттар технология мен қару-жарақтың баяу дамуы кезінде қабылданғанымен, олар әлі де қауіпсіздік мәселелері мен алаңдаушылықтарына қолданылуы мүмкін. Химиялық қаруды және кибершабуылдарды қолдану мысалдарын ескере отырып, мұны халықаралық әдет-ғұрыптық құқықты қолдану арқылы қолданыстағы құқықты күшейту қажеттілігі ретінде түсіндіру мәселелеріне байланысты халықаралық құқықтың кейбір нормаларының әлсіздігінің дәлелі деп санауға болады. Сондықтан, мемлекеттер тәжірибесі мен ғалымдардың қосқан үлесіне байланысты халықаралық құқық бейбіт тәртіпті қамтамасыз етуге немесе жаңа технологиялар мен қару-жарақ жасауға тән қауіп-қатерлерді болдырмауға көмектесуге қабілетті емес деп айту қиын.

Түйін сөздер: Халықаралық құқық, қару-жарақ, технология, кибершабуылдар, күш қолдану, халықаралық әдет-ғұрып құқығы.

Ж.И. Ибрагимов[1], Т.С. Асанова[2]

[1]Л.Н. Гумилева Евразийский национальный университет, Астана, Казахстан

[2]Astana IT University, Астана, Казахстан

Международное право и его отклик на современные угрозы безопасности, связанные с развитием вооружений и технологий

Аннотация. Появление новых технологий, таких, как нанотехнологии, кибертехнологии, космические и беспилотные системы, и их быстрое развитие оказали влияние на существующие нормы международного права, и наоборот, благодаря достижениям в области технологий

вооружений. Правовое урегулирование таких ситуаций происходит через толкование «старого» международного права и применение к новой ситуации или, при необходимости, через введение в действие нового права. В некоторых случаях действующее международное право может быть применимо к нему посредством расширения, в случае необходимости, нового толкования международных конвенционных норм в качестве аналогов обычного международного права. Несмотря на то, что некоторые международные договоры были приняты во времена медленного развития технологий и видов вооружений, они, тем не менее, по-прежнему могут быть применимы к вызовам и проблемам угроз безопасности. Учитывая примеры применения химического оружия и кибератак, это можно считать свидетельством слабости некоторых норм международного права из-за проблем толкования как необходимости усиления действующего права путем применения норм обычного международного права. Поэтому трудно утверждать, что международное право не способно обеспечить мирный порядок или помочь избежать угроз, присущих новым технологиям и развитию вооружений, из-за практики государств и вклада ученых.

Ключевые слова: международное право, вооружение, технологии, кибератаки, применение силы, международное обычное право.

References

1. McLaughlin R., Nasu N. Introduction: Conundrum of New Technologies in the Law of Armed Conflict // New Technologies and the Law of Armed Conflict. – Asser Press, 2014. – P.1-20.

2. Margules P., Sovereignty and cyber-attacks: technology's challenge to the law of state responsibility // Melbourne Journal of International Law. – 2013. – Vol. 14. – P. 496-519.

3. Boothby, W.H. Weapons and the law of armed conflict. – Oxford University Press, 2nd edn, 2016. – 464 p.

4. Henckaerts, J-M., Doswald-Beck, L. Customary international humanitarian law, ICRC. – Cambridge University Press, 2005. – 689 p.

5. Coleman S. Ethical challenges of new military technologies in Nasu, N., McLaughlin, R. (eds) // New Technologies and the Law of Armed Conflict. – Asser Press, 2014. – P. 29-42.

6. Joyner, D.H. International law and the proliferation of weapons of mass destruction. – Oxford University Press, 2012. – 402 p.

7. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC), 13 January 1993.

8. Fidler D.P. The meaning of Moscow: «non-lethal» weapons and international law in the early 21st century // International Review of the Red Cross. – 2005. – Vol. 87(859). – P. 525-552.

9. Dando M. The danger to the chemical weapons convention from incapacitating chemical. First CWC Review Conference Paper. No. 4, University of Bradford, 2003. – 252 p.

10. Universal Declaration of Human Rights, Article 3, GA Res 217A (III), UN Doc. A/810, 1948; International Covenant on Civil and Political Rights, Articles 4 and 6, 19 December 1966, UNTS, Vol.999.

11. Valeriano, B., Maness, R.C., Cyber war versus cyber realities. cyber conflict in the international system. – Oxford University Press, 2015. – 288 p.

13. Charter of the United Nations, 26 June 1945.

13. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US), Merits, Judgment, 27 June 1986, ICJ Reports 1986.

14. Legal consequences of the construction of wall in the occupied Palestinian territory, Advisory Opinion, 9 July 2004, ICJ Reports 2005.

15. Waxman M.C. Cyber-attacks and the use of force: back to the future of Article 2(4) // The Yale Journal of International Law. – 2011. – Vol. 36. – P. 421-457.

16. Roscini, M. Cyber operations and the use of force in international law. – Oxford University Press, 2016. – 336 p.

17. Green, J.A. (Ed.). The regulation of cyber warfare under the jus ad bellum // Cyber Warfare. A Multidisciplinary Analysis. – Routledge Taylor & Francis Group, 2015. – P. 1-6

18. Dinniss, H.H. Cyber Warfare and the Laws of War. – Cambridge University Press, 2012. – 353 p.

19. Schmitt, M.N. (gen. ed.) Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations. Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. – Cambrdige University Press, 2017. – 302 p.

20. UN GA Doc. 'Role of science and technology in the context of security, disarmament and other related fields', A/53/576, November 18, 1998.

21. Russia's «Draft Convention on International Information Security» (2012). A Commentary. http://www.conflictstudies.org.uk/files/20120426_csrc_iisi_ commentary.pdf (accessed 15.12.2022).

Black's Law Dictionary, http://thelawdictionary.org (accessed 01.12.2022).

23. HPCR, Manual on International Law Applicable to Air and Missile Warfare, http://www.ihlresearch.org/amw/manual/section-a-definitions/weapon (accessed 20.12.2022).

24. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, ICJ Reports.

25. The ILC Draft Article on Responsibility of States on Internationally Wrongful Acts, 2001.

26. Green, J.A. Disasters Caused in Cyberspace in Breau, S.C., Samuel, K.L.H. (eds), Research Handbook on Disasters and International Law. – Edward Elgar Publishing, 2016. – P. 406-427.

27. Corfu Channel case (UK v Alb.), 1949 ICJ 4 (9 April).

28. Graham, D.E. (2010). Cyber threats and the law of war // National Security Law and Policy. – 2010. – Vol. 4. – P.87-102.

Information about authors:

Ibragimov Zh.I. – Doctor of Law, Associate Professor, L.N. Gumilyov Eurasian National University, 2 Saptayev str., Astana, Kazakhstan.

Assanova T.S. –Master of Law, Senior Lecturer, Astana IT University, 55/11 Mangilik Yel avenue, Astana, Kazakhstan.

Ибрагимов Ж.И. – заң ғылымдарының докторы, Мемлекет және құқық теориясы мен тарихы, конституциялық құқық кафедрасы қауымдастырылған профессоры, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Сәтпаев көш., 2, Астана, Қазақстан.

Асанова Т.С. – заң ғылымдары магистрі, Халықаралық құқық, Astana IT University, Креативті индустрия мектебі, Мәңгілік Ел даңғылы, 55/11, Астана, Қазақстан.