DOI: https://doi.org/10.24833/0869-0049-2022-2-85-100

Research article
Received 3 March 2022
Approved 14 June 2022

Ara YEREMYAN
Russian-Armenian University
123, Hovsep Emin, Yerevan, Republic of Armenia, 0051
ara_yeremian@yahoo.com
ORCID: 0000-0001-9494-9943

Lilit YEREMYAN
Russian-Armenian University
123, Hovsep Emin, Yerevan, Republic of Armenia, 0051
lilityer@gmail.com
ORCID: 0000-0002-5127-3776

INTERNATIONAL LAW ISSUES OF CYBER DEFENSE

INTRODUCTION. *The world has many times faced cardinal changes triggered by technological development. Creation of the Internet and the emergence of the artificial intelligence have become the major trend of the ongoing changes with the significant potential to affect all spheres of live, including the military affairs and the geopolitical phenomena in general. In this paper, in particular, we discuss the opportunities and challenges of the rapid technological development in the defense sector in the context of globalization. The pace and the nature of changes in defense dictate the necessity to analyze the current and future challenges of our digitized age in search of adequate and timely legal and strategic practical solutions. Cyber means of warfare are the weapons of the present. Over the past decades, cyber means of warfare have been frequently used against states in the context of international and non-international armed conflicts, as well as outside of such context. Thus, the fundamental scientific questions that arise are the following:*

a) are the current legal regulations at international and national levels sufficient to address all the challenges caused by the spillover of armed conflicts into the virtual domain and by the future advancement of cyber weapons, and

b) are the current cyber weapons or those of the future capable of changing the nature of "war" described by General Carl von Clausewitz yet in the 19th century as a violent method of forcing its political will by one party of the conflict to the other.

We have analyzed the above-mentioned questions in the light of the cyber weapons, which already exist and are being used for military purposes, in the light of possible advancement of cyber weapons and integration of AI into them, as well as in the light of the Big Data management. We have reflected on the dangers, which the smart and entirely data driven world would face, from legal and geopolitical perspectives, through the several possible scenarios of development, emphasizing, in particular, the probable military (defense) aspect of data management. While most frequently the specific problems of application of International Law to the traditional cyber warfare situations become subject for academic debates and discussions, we stress the necessity to also analyze the legal and practical implications of further advancement of cyber weapons, as well as the necessity to consider the role of Big Data management in changing the nature of war and, consequently, also the applicable legal solutions.

MATERIALS AND METHODS. *The works of academics and international scholars in the field of international law and, specifically, international humanitarian law, and military theorists, as well as international treaties, commentaries to international treaties, and national cyber defense and cyber security strategies comprise the theoretical basis for*

the current paper. The research has been conducted via general and specific scientific methods of cognition, in particular the dialectical method, comparative legal method, method of interpretation, as well as methods of deduction, induction, analysis, synthesis, and others.

RESEARCH RESULTS. *The ongoing changes taking place in the world have resulted in a situation, when cyber domain is considered one of the traditional war domains. In this context the international community is now debating more flexible interpretations of international legal regulations in order to most efficiently address the new reality. It is also important that states at national level undertake measures to timely and adequately address the challenges already created and those that potentially may take place as a result of the globalization along with the rapid evolution of the cyber technologies and their military use. In the current article we conclude that the categories of the present generation of cyber weapons are lawful. However, the future developments in cyber weapon technologies, as well as the possible quasi-military implications of Big Data management raise many theoretical and practical questions deserving attention. The efforts of the international community and individual states in the field of legal regulation of cyber technologies should be directed toward creating guarantees that the products of the technological development are used for the benefit of humankind. As one of such measures The Authors indicate national cyber security and cyber defense strategies, which according to the Authors, should be elaborated giving due consideration to the possible future developments.*

DISCUSSION AND CONCLUSIONS. *In this paper we analyze the peculiar features of evolution of the world in the 21st century and argue that wars are not static and autonomous phenomena isolated from the global context and all the changes taking place in the world. In particular, we address one of the most popular debates among the scholars in the field of military affairs concerning the issue whether the nature of war has changed or will change overtime, referring to Carl von Clausewitz's thoughts. With regard to the current generation of cyber weapons, we conclude that even if they might prima facie seem to be inherently indiscriminate (such as, for example, nuclear weapons) in reality cyber weapons are not per se indiscriminate, but rather are weapons with a very high potential of being used indiscriminately or in violation of the principle of discrimination. However, the high potential of indiscriminate use of cyber weapons does not outlaw the cyber weapons as such. We also agree with the widely accepted opinion that the cyber weapons, which are currently used, are sufficiently regulated by the International Law. At the same time, the future tendencies for advancement and improvement of military cyber technologies, inter alia, via integration of artificial intelligence, may seriously call into question the possibility of their application in compliance with the international legal regulations. Finally, the possible scenarios of advancement of Big Data management have led us to the conclusion that big data management per se has the potential of being used as a weapon with less lethal or even non-lethal consequences, however equally effective in enforcing one's policy as the traditional weapons or potentially kinetic cyber-weapons. If big data analysis at its current stage of development does not produce very accurate predictions, the well-distributed and structured informational flow in the cyber domain is capable of influencing and manipulating behaviours. In such case if Big data monopoly (including both: hardware and software) vests in one of several actor, it could drastically change the nature of war by making the element of violence redundant and consequently alter the geopolitical balance. One of the measures for early response to future challenges, in our opinion, could be through reflecting on lex ferenda in cyber security and cyber defence national strategies. From the analysis of the content of different strategies we could conclude that most states acknowledge cyberspace as a military domain like land, air or maritime, analyse the main specific characteristics of current generation of cyber weapons, and set state objectives and action plan for cyber offense, cyber defense and cyber deterrence respectively. While the future advancement of cyber means of warfare and the quasi-military dimension of the big data management seem to be overlooked by states in general.*

KEYWORDS: *Globalization, technological development, military technologies, cyber weapons, cyber warfare, cyberspace, artificial intelligence, Big Data, international law, international humanitarian law, cyber defense, defense strategies*

FOR CITATION: Yeremyan A., Yeremyan L. International Law Issues of Cyber Defense. – *Moscow Journal of International Law.* 2022. No. 2. P. 85–100. DOI: https://doi.org/10.24833/0869-0049-2022-2-85-100

The authors declare the absence of conflict of interest.

DOI: https://doi.org/10.24833/0869-0049-2022-2-85-100

Исследовательская статья
Поступила в редакцию: 13.03.2022
Принята к публикации: 14.06.2022

Ара Владимирович ЕРЕМЯН
Российско-Армянский Университет
Овсепа Эмина ул., д. 123, Ереван, 0051, Республика Армения
ara_yeremian@yahoo.com
ORCID: 0000-0001-9494-9943

Лилит Араевна ЕРЕМЯН
Российско-Армянский Университет
Овсепа Эмина ул., д. 123, Ереван, 0051, Республика Армения
lilityer@gmail.com
ORCID: 0000-0002-5127-3776

МЕЖДУНАРОДНО-ПРАВОВЫЕ ВОПРОСЫ КИБЕРОБОРОНЫ

ВВЕДЕНИЕ. *Наш мир неоднократно подвергался кардинальным изменениям в результате технологического прогресса. Создание интернета и развитие искусственного интеллекта стали основной тенденцией происходящих изменений со значительным потенциалом воздействовать на все сферы жизнедеятельности, включая военные вопросы и геополитические явления. В данной статье мы, в частности, обсуждаем возможности, создаваемые стремительным технологическим развитием в оборонном секторе в контексте глобализации, а также возникающие в связи с этим вызовы. Темпы и характер изменений, происходящих в сфере обороны, диктуют необходимость проанализировать существующие и будущие вызовы нашей информационно-цифровой эпохи, в поисках адекватных и своевременных правовых и стратегических практических решений.*

МАТЕРИАЛЫ И МЕТОДЫ. *Теоретической основой данного исследования послужили работы зарубежных ученых в области международного права и, в частности, международного гуманитарного права, военных теоретиков, а также международные договоры, комментарии к международным договорам, и национальные стратегии различных стран по вопросам кибероборонны и кибербезопасности. Исследование было проведено с помощью общих и специальных научных методов познания, в частности, посредством диалектического метода, сравнительно-правового метода, метода толкования, а также методов дедукции, индукции, анализа, синтеза и других.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *В результате происходящих в мире изменений сложилась такая ситуация, при которой кибердомен рассматривается в качестве одного из традиционных пространств войны. В данном контексте международное сообщество обсуждает более гибкое толкование международно-правовых регуляций в целях обеспечения наиболее эффективной реакции на новые реалии. Важно также, чтобы и на государственном уровне были предприняты меры для своевременного и адекватного реагирования на уже существующие вызовы и на те вызовы, которые потенциально могут возникнуть в результате глобализации с параллельно происходящим стремительным развитием кибертехнологий и их военным применением. На данном этапе, это, как минимум, подразумевает также необходимость разработать эффективные национальные стратегии обороны, которые будут включать в себя, inter alia, регулирование киберпространства с компонентами кибернаступления, киберзащиты и киберсдерживания. С этой точки зрения, на наш взгляд, чрезмерно либеральный подход в рамках стратегий кибероборонны и кибербезопасноти должен быть пересмотрен в свете рисков и возможных вызовов, обусловленных продолжающимся развитием военных кибертехнологий и внедрением искусственного интел-*

лекта. Мы приходим к заключению, что кибероружие является оружием настоящего, а не будущего. И категории настоящего поколения кибервооружений правомерны. Усилия международного сообщества и отдельных государств в сфере правового регулирования кибероружия должны быть направлены на создание гарантий для того, чтобы результаты дальнейшего технологического развития применялись во благо человечества.

ОБСУЖДЕНИЕ И ВЫВОДЫ. *В рамках данного исследования мы анализируем особенности информационно-цифровой эволюции нашего мира в XXI веке и утверждаем, что войны не являются статичным и автономным феноменом, изолированным и выдернутым из глобального контекста, а прямо или опосредованно зависят от происходящих в мире изменений. В частности, мы рассматриваем один из наиболее обсуждаемых в военной науке вопрос, изменился ли характер войн в течение времени, обращаясь к идеям Карла фон Клаузевица.*

Далее мы анализируем, как развитие военных технологий и, в частности, киберсредств ведения войны, регулируется в рамках международного права.

В итоге, если настоящее поколение кибервооружений в достаточной степени регулируется международным правом при применении более гибкого толкования международно-правовых положений, очевидно, что будущие тенденции развития и совершенствования кибертехнологий, в том числе и путем интегрирования искусственного интеллекта, могут значительно изменить характер войн и логику геополитического расклада. Наконец мы обсуждаем возможные сценарии эволюции международного права, а также анализируем государственную практику по регулированию кибероборонs посредством национальных стратегий обороны.

КЛЮЧЕВЫЕ СЛОВА: *глобализация, технологическое развитие, военные технологии, кибервооружения, кибервойна, киберпространство, искусственный интеллект, международное право, международное гуманитарное право, кибероборона, стратегии обороны*

ДЛЯ ЦИТИРОВАНИЯ: Еремян А., Еремян Л. 2022. Международно-правовые вопросы кибероборонs. – *Московский журнал международного права.* №2.. С. 85–100. DOI: https://doi.org/10.24833/0869-0049-2022-2-85-100

Авторы заявляют об отсутствии конфликта интересов.

"When a young man in Siena, I saw how a couple of builders, after five minutes argument, replaced a thousand-year-old system for moving granite blocks by a new and more practical arrangement of the tackle. Then and there I knew - the old age is past and a new age is here."
(from The Life of Galileo by Bertolt Brecht).

1. The Features of Evolution in the New Age

Throughout thousands of years our world has several times passed through global cardinal changes triggered by drastic scientific or technological development, new discoveries and mindset or thinking transformation for the given time-period. Every time such change was coupled with resistance, opposition; political, ethical, religious, economic, social or legal discussions of different content and severity; geographical, temporal and qualitative asymmetry in acknowledgement of the new reality and implementation of the new knowledge. Today we are lucky to not just experience but also have the opportunity to become a part of yet another global, almost civilizational change taking place in and with the world. From this perspective, the 21st century evolution is unique by three main aspects: 1. the rapidity of the development, 2. the nature of the actors causing the change, 3. uncertainty and the inner seeming controversies and unity of the phenomena comprising this change. Instead of the gradual progress of the past centuries we are going through the age of rapid changes touching all spheres of life from science and technology to governance and social life. What was science fiction yesterday has already become reality, and what seems science fiction today will, most likely, very soon constitute the everyday life. The states, which have embraced this reality, nowadays race for not just being ready for the future, but also for having own input in this process of rapid evolution and creating the future.

Not even 50 years ago the doctrine of public international law viewed states as the only subjects of international law, the Statute of the International Court of Justice uses the wording "civilized states" (article 38). The concept of "civilized states" is currently absolutely archaic. Peoples fighting against racist régimes in the exercise of their right of self-determination, state-like entities, and international intergovernmental organizations are overall recognized as subjects of international law, and the academia is debating on international legal personality of non-traditional actors such as transnational corporations, international NGOs, individuals and even organized armed groups. A few decades ago we were still living in a truly bipolar world. In the new reality the small states which will fully embrace the technological progress, becoming a part of it, will have good chances of influencing the global changes yet to take place in the world. Transnational corporations or even individuals nowadays also have the opportunity of causing global changes.

With the current state of things globalization has become unavoidable. State borders have lost their previous meaning. In our new age Covid 19 has more speedily changed the nature of globalisation, taking it to a new - virtual level. Events which previously were traditionally being organized live had to switch to online format, distance learning has become the main teaching method, arts and music have to utilise the opportunities of new technologies, services that were hesitant to use online platforms, such as justice or banking, now have to timely adapt to the new reality. These tendencies consequently result in higher virtual mobility. Now we deal with a form of globalisation, where cyber technologies and the Internet play *the* most important role, in which states de facto have very limited authority or control and where the behaviour of individual units, the patterns of their interaction among each other and the outcome of such interaction cannot be predicted with certainty. With all these transformations taking place in the world, we can firmly conclude that the old age is past and a new age is here. In this new age especially the rapid advancement of the cyber world, nearly every actor, be that an individual, a group or a small state, is theoretically capable of obtaining real power and even having geopolitical influence. The physical or geographical position of the actors or the state borders is no longer the determinative factor for success. The pace of changes in all spheres and at all levels makes the traditional solutions inapplicable. The extraordinary levels of interconnectedness make the behaviour of separate actors less predictable. And our duty is to try to perceive and conceptualize the new reality, embrace the uncertainty and follow the probable patterns, finding creative solutions, learning lessons, converting the challenges into opportunities. Not surprisingly, this new state of things has influenced and modified all spheres of our life, including the defense sector.

2. On the Nature of War

Military affairs and wars are not static and autonomous phenomena isolated from the global context and all the changes taking place in the world. Wars are dynamic in nature and the general tendencies even allow us to conclude that wars on the one hand and globalisation and science-technological development on the other hand are interdependent. Thus, globalisation and technological advancement drastically influence the character of armed conflicts, at the same time the defense priorities and challenges are the most dominant incentives for technological advancement and further globalisation. Interestingly one of the most popular debates among the scholars in the field of military affairs concerns the issue whether the nature of war has changed overtime. Prussian General Carl von Clausewitz's work titled 'On War' [Clausewitz 1984] represents one of the most valuable pieces on this topic and the main source and reference for debate. In this book the General argues that the nature of war that is to say its' essence is constant, while the character of war, that is to say how the wars are being conducted, is changing adapting to the context. Carl Von Clausewitz, thus, describes wars as a violent method of forcing its political will by one party on the other, meaning that war is not an end in itself, but rather "an act of policy or a continuation of a policy by other means" [Clausewitz 1984:87]. He further analyzes that the intention of parties in wars is not the destruction in and of itself, but rather making the enemy defenseless or putting the enemy in a situation when this danger becomes very probable [Clausewitz 1984:77]. Consequently defining the nature of war as comprising the 'paradoxical trinity' of hostile emotions, laws of probability and an instrument of policy as the only rational element in this trinity [Clausewitz 1984:89], concluding that the essence of war doesn't change depending on external factors. Some scholars and experts agree with the Clausewitz's analysis, while others argue pointing out the features, which have changed the nature of modern wars. [Lye Chee Wei: 2020; Pappila 2008:69-73; Kaldor 2012: 268] While this debate is essential for understanding the core

motives and elements of war from the theoretical perspective, in practical terms what makes difference is that the wars are evolutionizing with the world, due to gradual transformations the main variables of modern wars are different from those that were acknowledged traditionally, and the new tendencies might completely change the logic of wars, regardless of whether we call it a change of 'the nature of war' or 'the character of war' or anything else. Throughout the history until the second half of the XX century the perception of wars was limited to armed confrontation between two or more states. We can follow this logic also in the text of the four Geneva conventions of 1949[1] stipulating legal regulations for international armed conflicts, which uses the wording and is applicable to 'High Contracting Parties', with only a very weak acknowledgement of the necessity to regulate also the conflicts not of an international character in Common article 3. Addressing the process of decolonization and emergence of nations fighting for their right of self-determination, as well as the drastic rise in the number of armed conflicts in which non-state actors were a party to the conflict, with the adoption in 1977 of the two Additional Protocols to the Geneva Conventions[2] the International Humanitarian Law (IHL) has expanded the definition of the international armed conflicts to cover also situations in which 'peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination, as enshrined in the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations'[3], as well as expanded the concept of armed conflicts to firmly include along with international armed conflicts also armed conflicts between a state and a non-state actor (organized armed group)[4], stipulating specific regulations for such non-international armed conflicts. At the same time, the nature of warriors has also changed. If in the past wars were fought by state soldiers, nowadays outsourcing of military functions, especially through the private military and security companies, have become a rule. The global war-on-terror announced by George W. Bush[5] in response to the terrorist attack of 9/11 and the action taken based on this declaration eventually blurred the lines between combatants and non-combatants. This resulted in emergence of new characteristics of warfare: namely asymmetry and application of unconventional tactics and strategies. The military transformation touched also the traditional perception of the physical domain of the armed conflicts. Now in line with the classical understanding of battlefields in air, water and land, the virtual/cyber domain is already acknowledged as a new form of battlefield. The persistent changes taking place over the last several decades lead to new interpretations of international legal regulations in order to most efficiently adapt them to the new forms of armed conflicts prevailing in the globalized world.[6] Last but definitely not the least, the need to adapt to the new features of armed conflicts, the possibilities of scientific and technological advancement, especially after invention of the Internet, promoted the rapid advancement of new means of warfare, such as cyber weapons, capable of changing the whole logic and perception of wars.

3. International-legal Regulation of New Means of Warfare

Advancement of new military technologies is often perceived negatively, with assumption that it would only add on the suffering and destruction, despite the fact that in some cases the diligent use of

[1] Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (Geneva 1949), Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Geneva 1949), Convention (III) relative to the Treatment of Prisoners of War (Geneva 1949), Convention (IV) relative to the Protection of Civilian Persons in Time of War (Geneva 1949).

[2] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I) date 8 June 1977, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II) dated 8 June 1977.

[3] AP I. Art. 1. Clause 4.

[4] AP II. Art. 1. Clause 1.

[5] President Bush's address to a joint session of Congress and the nation. – *The Washington Post.* September 20, 2001. URL: https://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html (accessed 28.02.2022).

[6] Thus, the 1952 commentaries of Geneva conventions were replaced by the modified analysis and interpretation of treaty regulations in 2016, not mentioning the significant amount of other doctrinal interpretations reflecting the new realities of armed conflicts.

new means of warfare could even minimize the destructive consequences of war. This, of course, leaves the relevant specialists and experts in the field with a necessity to analyze the probable scenarios of use of these new weapons and adequacy of the existing international-legal regulations. In some cases the outcome of such analysis may be determination of the necessity to limit and regulate the use of a weapon at hand (for instance as it was the case with incendiary weapons[7]), or the necessity of strict prohibition of the relevant means of warfare (like it was the case with chemical and biological weapons[8]), or in some cases such analysis would lead to the conclusion that there is no necessity of special restrictions or prohibition of the relevant weapons, or that the existing regulations are sufficient if interpreted flexibly through soft law to take into account the specific characteristics of the new weapons[9]. However, it is also possible that one day due to the extraordinary pace of the technological development and constant rapid modifications of weapons technologies any existing or even emerging legal regulation will be outdated.

At international level the prohibition of weapons takes place either via elaboration of a treaty directly prohibiting or limiting the use of a certain weapon or through the general principles of IHL envisaged in 1977 AP I, which prohibit weapons (without specifically mentioning the type of weapon) of a nature to cause superfluous injuries or unnecessary sufferings (principle of prohibition of superfluous injuries and unnecessary sufferings), as well as weapons that are by nature (inherently) indiscriminate (principle of discrimination) [Customary International Humanitarian Law...2005:237-250][10] The principle of prohibition of superfluous injury and unnecessary suffering is aimed at protection of combatants from suffering and injuries that are redundant in terms of gaining military advantage or for which there is no military necessity. This principle outlaws the use of methods, as well as means of warfare, which per se due to their characteristics cause superfluous injuries or unnecessary sufferings to combatants[11]. While the principle of discrimination is aimed at protection of the civilian population and comprises of two elements: a/ prohibition of deliberate attacks on civilians or civilian objects and b/ prohibition of indiscriminate attacks [Dinstein 2010:124-128]. Indiscriminate attacks are attacks, which are not directed against a specific military objective, regardless of the weapon used (i.e. indiscriminate shooting), as well as attacks with inherently indiscriminate weapons.[12] Now, in terms of regulation of means of warfare this last element is the one posing interest for our discussion. Article 51 clause 4 of AP I defines indiscriminate attacks with inherently indiscriminate weapons as attacks which employ a method or means of warfare which cannot be directed at a specific military objective, or attacks which employ a method or means of warfare the effects of which cannot be limited as required by AP I. So, just as in case of the principle of prohibition of superfluous injuries and unnecessary sufferings, the principle of discrimination also emphasizes the nature or the technical characteristics of a weapon as a necessary precondition for the per se unlawfulness of a weapon and thus its ban under IHL. Now it becomes obvious that in most cases the indiscriminate nature of the attack is a result of the way of using the weapon rather than its technical characteristics. Moreover, in our opinion, up to this point the only means of warfare which might be considered meeting the characteristics of an inherently indiscriminate weapon is biological weapon, the ef-

[7] The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to de excessively injurious or to have indiscriminate effects of 1980 as amended on 21 December 2001 (CCW). Protocol III on Prohibitions or Restrictions on the Use of Incendiary Weapons.

[8] Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction of 13 January 1993; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction of 10 April 1972.

[9] Until now this has been the approach of regulating cyberspace with two major analysis on application of IHL in particular and public international law in general to cyber operations: [Tallinn Manual…2013; Tallinn Manual 2.0…2017].

[10] For the principle of discrimination see also: articles 48 and 51 of AP I. For the principle of prohibition of superfluous injuries and unnecessary sufferings: article 1 clause 2 and article 35 clause 2 of AP I; Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons. 1996. Para.78. URL: https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (accessed 28.02.2022).

[11] An example of weapons causing superfluous injuries and unnecessary sufferings is any weapon the primary effect of which is to injure by fragments which in the human body escape detection by X-rays, prohibited under Protocol on Non-Detectable Fragments (Protocol I) to CCW, and the logic behind that the characteristic of non-detectability of fragments in hors de combat is not necessary for gaining military advantage.

[12] AP I. Art. 51. Clause 4.

fects of which cannot be predicted or limited, consequently inevitably affecting combatants and civilians without distinction. While other weapons, including those, which might *prima facie* seem to be inherently indiscriminate (such as, for example, nuclear weapons) in reality are not *per se* indiscriminate, but rather are weapons with a very high potential of being used indiscriminately or in violation of the principle of discrimination, which however, does not outlaw the weapon itself. The mentioned two approaches in legal regulation of weapons, namely treaty regulation and customary IHL principles, are in fact complimentary to each other: the treaties are binding for the parties of the relevant treaty (unless its provisions are qualified as norms of customary international law) and represent the political will of the state-parties to regulate or completely prohibit a concrete weapon or a specific category of weapons. While customary IHL principles, binding for all states, are, inter alia, aimed at prohibiting all weapons with technical characteristics that would not allow using them in compliance with the mentioned principles. However the wording of AP I provisions and their interpretation, as shown above, could lead us to a conclusion that a very limited number of weapons would fall under the prohibition in the context of the given principles. This conclusion might be disappointing and questioning the effectiveness of prohibiting weapons via customary IHL principles in practice. However their role is significant in terms of evolution of IHL as the ideological basis for all legal discussions concerning the means and methods of warfare, as well as an inspiration for elaboration of treaties on different means of warfare. This mentioned mission of the IHL cornerstone principles should not be underestimated.

4. The International-legal Regulation of Cyber Means of Warfare

The evolution in military technologies has been very significant in the recent decades, modifying different traditional weapons and bringing forward new ones, of which our focus will rest on cyber means of warfare for the following main reasons: a/ the basic principle of action in cyberspace is interconnectedness or probable interconnectedness of everything, which precisely reflects the essence of the nature/world ecosystem (Barry Commoner's first law of ecology), b/ cyberspace is a reflection of the global changes, as well as their cause, c/ cyber means are the fastest developing technological field of all times, d/ cyber means of warfare are truly capable of changing the nature of wars and the logic of defense management. For any implications on the impact of the use of cyber weapons and the issue of their lawfulness, it is first necessary to reflect on their essence and the differences compared to other more traditional categories of weapons.

After around 40 years since one of the most, if not the most, influential inventions of all times – the Internet, in 2021 the number of active Internet users in the world has reached approximately 4.6 billion according to some estimates. Internet has entered all aspects of our lives at micro and macro levels. All global and state infrastructures around the world, including military infrastructure, as well as devices and systems at personal or collective levels, with every year become more and more cyber-dependent. State defense and security relies almost completely on the information technologies. Just to illustrate this it is sufficient to mention that already by 2010 around 98% of all U.S. government communications, obviously including significant flows of military communications was being transferred through civilian networks [Talbot Jensen 2009-2010:1542]. One of the most striking characteristics of our digital age is blurred between public and private, defense sector and civil networks, lawful and unlawful, between the real world and the cyber world. Currently cyberspace is being recognized by most states as one of the standard domains for armed conflicts, like land, air and maritime. Cyberspace could be defined as the computers, mobile devices, and users thereof altogether, using the Internet to connect [Danelyan, Gulyaeva 2020:44-53]. The attractiveness of the military use of cyberspace can be explained by a number of obvious factors. Development of cyber means of warfare is possible with limited recourses and it is feasible to almost every individual, group of individuals or state. Cyber means of warfare create opportunities for weapons with a very wide variety of intensity and impact, starting from non-lethal and non-destructive malware affecting the target system without directly harming it, to potentially lethal or destructive cyber agents capable of physically damaging a system or causing lethal results. At the same time the consequences of the use of cyber weapons do not necessarily depend on the level of their lethality, even the use of low potential cyber means could lead to major disruptions in social or state life, thus, becoming sufficient for forcing the adversary to act in this or that way. Additionally, it is extremely difficult if not impossible to trace and detect the source of the attacks through cyberspace, and due to the decentralized and interconnected nature of cyberspace it is even more difficult to confirm attribution

of attack to this or that state, organization or person. The global network is also much more liberal with states having very little control over it. Besides, even though legal experts in the field overall agree that the existing international legal norms in general and IHL provisions in particular are appropriately regulating the cyber-warfare domain, it would be fair to state that there are obvious gaps in applicable legal provisions or their interpretation with regard to their application to the use of cyber means. This makes it easier to avoid responsibility. It is, thus, undisputable that cyber domain, when we are speaking of its military use, shall be taken by states as seriously as all traditional domains. Moreover, it must be taken into consideration that cyberspace is the only domain that is heavily interlinked with land, air and maritime, often even highly influencing military operations in the mentioned traditional battlefields via the use of cyber-dependent weapons, software-controlled systems.

Cyber warfare in essence constitutes an international armed conflict (IAC) or a non-international armed conflict (NIAC) or act (acts) conducted by cyber means in the context of an IAC or NIAC to achieve military objectives, including cyber-offence, cyber-defense and cyber-deterrence. Cyber means of warfare could be used in many different modes, such as deception, neutralization, manipulation, modification, infiltration, assault, cyber- raid, cyber-intelligence, etc. [Alford 2000:105]. There are myriads of scenarios how cyber means can be used to threaten, cause panic, facilitate gaining military advantage, including by disrupting the functioning of systems, or causing harm and destructions respectively to persons or objects. Compared to many traditional weapons cyber means of warfare have a very high potential of being used in violation of the principle of discrimination, which can be explained by two major factors: 1. even if the cyber operation is launched against a specific military objective, the incredible levels of interconnectedness of military and civil infrastructures may lead to unpredictable and unintentional penetration and spread of the malware into civilian networks, 2. the tendencies for asymmetric warfare and easy access to cyber means of warfare by individuals, groups and states, and the difficulties to trace the source or to find proof for attribution, make cyber means very attractive for merely anyone, including for the purposes of deliberately launching operations against civilians having the final aim of imposing of one's political will. No coincidence, that cyber means of warfare are often compared or referred to as weapons of mass destruction [Hatch 2018:43-61; Cirenza 2015; Shackelford 2009]. At the same time, it is worth mentioning that if planned and implemented professionally and with due diligence cyber means of warfare can be very precise in targeting specific military objectives in compliance with the principle of discrimination. Moreover, cyber means could in some cases provide an opportunity to target objects physical targeting of which with traditional weapons might otherwise be qualified as disproportionate (for instance, destruction of military databases under specific circumstances). There are myriads of scenarios of employing cyber means of warfare in the context of IAC or NIAC or outside of such context. Indiscriminately cyber weapons could be used, for example, against the healthcare system by modification of initial data and records or by temporary taking out of order the healthcare related electronic systems, which could cause tremendous harm and even put at risk people's lives. Cyber means of warfare could be used indiscriminately to attack banking system and depending on the scale, duration and intensiveness of the cyber operation it could cause panic among the civilian population and by its effects could even amount to terrorization of the civilian population, which is prohibited under IHL [Customary International Humanitarian Law…2005:8-11][13], without causing any tangible, physical damage to persons and objects. Cyber means of warfare have the potential of targeting nearly any critical infrastructure from power plants, oil and gas pipelines and chemical factories to water or electricity supply, due to the networked character of such infrastructures and their heavy dependence on the network for proper operation. Cyber weapons could be used to alter the aviation or marine services of a given state, causing chaos and destruction, loss of lives among the civilians, or to bring out of order the traffic lights causing mass road accidents. Along with indiscriminate use, cyber means can also be used to damage concrete objectives lawfully, such as military archives, or to alter command and control transferred through the military networks in order to affect military operations of the adversary, or to destroy a certain military objective physically, for instance by intercepting initial information about the preconditions for normal functioning of any system or device and manipulating the process of its opera-

[13] AP I. Art. 51. Clause 2.

tion via a cyber agent transferring false or modified data through the command-and-control server (e.g. changing the optimal temperature regime or the velocity of a substance) which eventually would result in damage of the target-object.

Cyber means in and outside of IAC or NIAC context have been commonly used for at least the last couple of decades. For example, the Stuxnet worm used to damage Iranian nuclear centrifuges, cyber means of warfare coupled with kinetic attacks in Syria, were among the most publicized cases of use of cyber means. Already in February 2016 the then Secretary of Defense Ashton Carter openly spoke about the United States using cyber means of warfare along with traditional weapons in military actions against Daesh[14], while the UK officials revealed the existence of a National Cyber Force, integrated with the regular military forces, only in 2020[15]. The deployment of cyber means as weapons by different states is, inter alia, evidenced by cyber-defense strategies of various states.

Not surprisingly, different aspects of international legal regulation of cyber weapons have been a matter of academic discussions for the past decades. In general terms, experts emphasize a number of problematic issues in the context of the use of cyber weapons. What kind of cyber operations outside of context of IAC or NIAC should be qualified as IAC or NIAC? Are the physical consequences or the kinetic component of cyber operations prerequisite for qualifying the operation as a military attack? Should the military electronic data be qualified as a military objective? Should the cyber forces be qualified as combatants? What is the level of organization for non-state cyber forces in the generally chaotic and decentralized cyber domain to be qualified as an organized armed group in the meaning of IHL? These and many other issues that represent only details concerning international legal regulation of cyber-weapons, are being regularly debated by experts with follow-up commentaries and interpretations comprising soft-law on the matter and being subject to periodic revision, modifications and updates in line with the new challenges of the use of cyber means uncovered overtime. What is very likely to be constant and not subject to change, however, is the overall lawful status of the use of cyber weapons. Despite the high potential of being used indiscriminately it is generally acknowledged that cyber weapons are not per se (inherently) indiscriminate and can be well used in compliance with the IHL principle of discrimination (while the lawfulness of their use is not questionable in the context of the principle of prohibition of superfluous injuries and unnecessary sufferings). On the other hand, there is no treaty ban or restrictions on cyber means of warfare. Concluding any such treaty in the future is not just objectively unrealistic, but also ineffective, due to the rapid evolution of cyber weapons and short lifespan of individual computer agents, as well as inexpedient, because such limitation would be binding only for states, putting the organized armed groups in a better position. So, summing up, cyber weapons are weapons of the present and they are lawful.

5. Current generation of Cyber Weapons and Tendencies of Cyber Evolution

Some of the features of the current generation of cyber weapons compared to traditional weaponry to be highlighted are the following: relative low cost, easy accessability, relatively high anonymity, with myriads of probabilities of behaviors, higher risks for civilian infrastructures, their production and circulation is outside of state control in the classical sense, usually their effectiveness depends on the knowledge of vulnerabilities of the military objective, they operate in accordance with the instructions inserted into the cyber agent/ code without or with little further human control, representing a myriad of different types of cyber-weapons with different potentials, constant and very rapid modification/ change of the cyber weapons. It is obvious that the ongoing quantization of things, including the rapid changes in the field, will alter also the general features of the cyber weapons in attempt to make them smarter and even more efficient than the current generation of cyber means. The outlined dominating tendencies of our new age in the world in general and in the field of weaponry in particular are higher autonomy with integration of AI, aspiration towards lower lethality risks with higher efficiency in achieving the final aim, and unconstrained imagination and creativity. At least this has been the approach with strongly

[14] In Fight Against ISIS, U.S. Adds Cyber Tools. – *NPR*. February 28, 2016. URL: http://www.npr.org/tem¬plates/transcript/transcript.php?storyId=468446138 (accessed 28.02.2022).

[15] Corera G. UK's National Cyber Force comes out of the shadows. – *BBC News*. November 20, 2020. URL: https://www.bbc.com/news/technology-55007946 (accessed 28.02.2022).

cyber-dependent autonomous weapon systems, in the context of which the technology development has reached the point when the prospect of employing killing robots in armed conflicts seems realistic to the extent that states are already intensively discussing and disputing the legal, technological, ethical and other aspects of such a scenario. Moreover, some experts see the possibility to perfecting the robots in the likeness of human beings or creating ethical autonomy: robots as intelligent, reasonable and compassionate as humans, which would facilitate to the reduction of destruction and losses in the course of armed conflicts [Arkin 2014:33-37]. Similarly we can outline certain patterns of cyber evolution, which might seem science fiction but only for the present moment. Integration of AI into cyber weapons is one of the most foreseeable trends. Smart cyber codes might be designed to learn not only from their previous experiences but also from the analysis of the environment and the context in which they should be employed uncovering even the indirect and not obvious links and connections which otherwise wouldn't be analysed and taken into consideration. At the same time the traditional methods of counteractions to neutralize harmful agents can become inefficient if the smart cyber weapon learns to modify itself. In such a case scenario it would be nearly impossible to stop or control it. For a better illustration we could compare such a smart cyber weapon with Covid 19. Based on the initial knowledge about the virus different vaccines were elaborated against it. However the virus has modified over time in order to survive, while the vaccines are still protective to some extent, however they are not as effective against the new variant of the virus. In the meantime, the transmissibility of the virus has increased and the consequences have become more severe. By analogy, the most challenging feature in this scenario would be the speed with which the e-code could become smarter and its possible spill over the infrastructures which were not intended to be targeted by the initial design of the given cyber weapon, making it much harder if not impossible to react. And this, of course, will raise the question whether our traditional approaches towards regulation of cyber weapons should also modify with the evolution, and whether the ex-post updates and changes in legal interpretations would be efficient for regulation of that specific threat.

Another pattern of cyber evolution could take us to a situation when big data management is used as a weapon with less lethal or even non-lethal consequences, however equally effective in enforcing one's policy as the traditional weapons or potentially kinetic cyber-weapons. Albert Einstein famously said 'information is not knowledge'. And this is true taken at an individual scale, however the concept of big data and the emergence of machine learning, big data management seem to challenge Einstein's proposition. Opinions like 'he who controls the information controls the world', 'whoever controls the web controls the world', 'the world is controlled by data' or 'data is the new oil' have become common recently, and in some sense they are not groundless. Every minute billions of people create huge amounts of content in the Internet either directly by sharing information via social networks or indirectly as a result of making transactions, through state records or in another way. Some of the information shared in the web is open, but there is also an enormous amount of information access to which is restricted based on different parameters: from sensitive personal information (like medical records, banking and financial information, etc.) to classified military information or data concerning operation of critical infrastructures. The size of the data is, thus, tremendous. But what is more important any piece of such information is rapidly changing and is directly or indirectly interconnected with many other pieces of information. The complex informational flood in itself is not possible to measure or process manually, and, certainly, it per se does not create knowledge. However unlimited volume for cloud storing and the machine learning technologies open not classical AI driven methodologies for conditionally speaking measuring the information flows and transforming information into knowledge. In fact, this transition from quantity to quality is not an extraordinary phenomenon, but one of the basic laws of dialectics that should not be neglected in the process of evolution.

The term big data could be interpreted as reflecting the size of information and its constantly growing nature, which is often described through the five V's of big data: volume, velocity, variety, veracity, value. It could also be interpreted as advanced technologies that are capable of analyzing and organizing the immeasurable volumes of unstructured information, and consequently extracting patterns which then become the basis for prediction of future behavior patterns [Chi 2017:1].

The new technology based analytics has created opportunities for a better, smarter, more tailored, and more effective decision making in many fields of life from public governance to different directions in the private sector. Not surprisingly, the states and technological giants have manifested unhidden enthusiasm for further rapid evolution of machine

learning and creating grounds and additional occasions for generating, collecting and processing more and more information by injection of internet dependence into almost all of our daily activities, and even into human minds. The invisible Internet is literally everywhere, causing transformation of values and forming a parallel cyber reality. At this point in time, though, it would be logical to defend Einstein's proposition on the transformation of information into knowledge since the current stage of machine learning development is far from its potential peak. Big data analysis, which technology is capable of nowadays, being the most accurate existing analytical tool is still is not representative of the reality. One of the underlying reasons is the number of people who are not active Internet users: around 3.3 billion people worldwide. Moreover, Internet presence does not always give comprehensive information depending on the behaviour of the Internet user in the web, especially with growing privacy concerns and raising awareness in this field. At the same time, often the information shared in the cyber domain reflects on the illusionary side of Internet users as people share only content which would put them into a more advantaged position rather than the content which represents the real nature of a given internet user. The most beautiful, smart or kind image or illusion of an Internet user may in reality represent a person with opposite characteristics, the most social and extravert person in the cyber domain with thousands of online connections may turn out to be an introvert in reality with only few friends. On top of all these natural and psychological factors that degrade the true picture in the cyber domain, the advancement of technology add on this by the use of fakes and deep fakes, which seem to be more utilized at a political rather than individual scale. As a result of employing of fakes, for example, the most popular political party or a public character in the cyber domain may turn out to be the least popular in the reality. Deep fakes could be used to make up non-existing reality. But the most interesting side of this is that sometimes such created illusions in the cyber domain are *per se* capable of influencing people's thinking and behaviours. In other words, even if big data analysis at its current stage of development does not produce very accurate predictions, the well-distributed and structured informational flow in the cyber domain is capable of influencing/ manipulating (rather than predicting) behaviours[16]. Now, big data and its analysis do not possess a kinetic component and at its current stage of development it definitely can't even be considered as a mean of warfare. Nevertheless, everything changes. It is no secret that along with the arms race, there is also a strong race in the cyber domain, including machine learning and big data management, between states and other stakeholders. This is paralleled with an incredible amount of information being added to the already existing unlimited pool of information every moment. Now let us imagine that at some point everything becomes entirely based and dependent on the web for all the people on our planet. Let us imagine that people are living in smart apartments and houses, dining in smart restaurants, driving smart cars, and that the technology has learnt to discriminate the false content from the real content and that it has learnt to accurately predict the human thought that precedes the behaviour. What if the information mined about every person gives an opportunity to even duplicate the given person in the cyber reality, to humanize cyber. All that a human being needs is just a smartphone attached to the body for convenience, which is, of course, nothing like our current smartphones. Let us imagine that just like it was the case with electronic signature, which over time became equivalent to the handwritten signature, the electronic image or a code of the person will become equivalent to physical presence. What if the states go entirely cyber for managing all infrastructures, for organizing national security, healthcare and the defense system of the country, and that only smart weapons are used for defense, no heavy artillery or traditional weapons, just like our generation is not using bows and arrows, swords and blunt weapons in the battlefields. What would the role of data be in such a reality? What dangers will the smart and entirely data driven world face? It seems that the probable military/ defense aspect of data management is sometimes being underestimated and ignored.

6. Geopolitical Alignment Scenarios in Cyber World of the Future

At the end of the day wars are fought for power, dominance (whether it's local, regional or global) and survival. It would be impossible to predict what would be the eventual outcome of such situation in

[16] For the analysis of the risks to the freedom of thought in general see [Yeremyan, Harutyunyan 2020].

terms of geopolitical alignment. One of the scenarios is that humans retain control over the cyber world and data management, in which case the possible outcomes would largely depend on the actors possessing the data management powers. Given that in the cyber world any single agent, be that an individual, a group of individuals, a small state or a group of states has certain chances for controlling the web. Big data monopoly (including both: hardware and software) could vest in one actor, drastically altering the geopolitical balance. This would mean dependence of all other stakeholders on this one actor with the cyber power. It could also mean that there would be no need for wars in a classical understanding, because the mere fact of possession of control over the web would be a sufficient tool for imposing the political will on other actors. Otherwise the consequences of confrontation could be unpredictable and disastrous: from shutting down all cyber dependent infrastructures or erasing all world data stored until the given moment to opening access for everyone to entire e-information, including classified information, sensitive personal data, etc. A more chaotic and violent future could be expected if the cyber power becomes concentrated asymmetrically in the hands of different individuals, transnational companies, organized armed groups, several big and small states. This would most likely result in continuous cyber race with actual use of cyber weapons for acquiring dominance, and could even reach the scale of selective extinction of groups of people based on various criteria, such as medical condition, ethnicity or race, preferences, profession or other. While a symmetric distribution of cyber power (software and hardware) between several major geopolitical players and establishing reasonable control over cyber-freedom of individual actors would create grounds for a comparatively organized and balanced world order. In a sense, cyber means are indeed similar to nuclear weapons, which can be disastrous, but could also play a significant deterrent role. On the other hand, cyber is conceptually different from nuclear weapons by its technical characteristics, specifically invisibility and per se non-lethality, as well as in terms of actors possessing this instrument or potentially having access to it. To put it simpler, it is much easier to establish control with regard to possession of nuclear weapons than cyber means, including big data management. In another scenario humans could be competing with the cyber. In a metaphorical or more philosophical-ethical context the competition would be over preserving the realness of the world and the souls of human beings. In more practical terms such competition could be reflected in a race between smart cyber technology trying to outpace the human capacities and humans trying to elaborate new smart cyber counter-means: pretty much like the race of a constantly mutating virus with humans in developing of effective vaccines. And then, probably, with the most science fictional scenario cyber would gain control over humans. Though, not very probable, but also not excluded, that the whole world population becomes cyber addicted, or, for example, a human-computer interface gets designed via which the smart computers would be dictating people the smartest and most accurate decision-making based purely on the big data analysis. In such a scenario, however, humans would still preserve their free will that would be occasionally used to 'revolt' the decisions prescribed by computers.

More globally and philosophically this discussion also makes us contemplate on what is the future world that we would want the next generations to live in. No doubts the advancement of cyber technologies and machine learning can improve our everyday life and make the world a better place if utilized in accordance in the universal human values. But our civilization must really decide on the red lines, which should not be crossed. Yes, big data may be eventually capable of making precise predictions and giving best advice for decision-making in all spheres of life, it could hold humans back from making mistakes and it could facilitate establishing high levels of order, certainty and predictability. But we must ask ourselves a question: is that the reality we would ever like to live in? Should humans strive to achieve a zero-mistake or close to a zero-mistake life at all, and especially at the cost of realness? Are we ready to sacrifice our souls and emotions for comfort and welfare? Leaving the ethical and philosophical aspects of the issue for another occasion and concentrating on the practical side, this journey into the probable future shows that cyber in general and data management monopoly (software and hardware), in particular, could in theory result in establishment of a unipolar alignment, or it could create chaos and destruction, but it could also have an opposite role: becoming an instrument for balancing and deterrence of violence. Now, returning to Carl Von Clausewitz's definition of war as a violent method of imposing the political will in the context of the probable cyber advancement, the conclusion would be that cyber is in fact capable of changing the very nature of wars, making the element of violence redundant and breaking the paradoxical trinity by extruding the emotional component.

7. Implications for the Evolution of International Law

With all this discussion on the present challenges and future implications, we could fairly conclude that now is the turning point. Our task in the context of cyber is to determine whether the given case at hand is specific, identify the ways in which it is new and analyze whether the theory and practice are adequate. The prohibition or otherwise changing the law to regulate a certain weapon at both international and national levels should take place after carefully assessing all arguments in order to avoid a situation of prohibiting a weapon, which in fact compared to traditional weaponry could have a higher potential of being used in compliance with cornerstone IHL principles, on the one hand, and on the other hand, to avoid a situation when technology bypasses human expertise to the extent that it becomes too late for imposing any regulations. With the use of cyber means, the question would be whether the danger of misusing cyber means now or in the foreseeable future is so big that a strict ban or a restrictive regulation is needed. And for this purpose classical cyber weapons (including the hypothetical possibility of development of smart cyber weapons) should be distinguished from Big data, even though as illustrated *supra* big data management at some point in time might really become equivalent to a non-lethal weapon. Further there should be a distinction between regulation of routine cybercrimes[17] and cyber means which could be used as weapons in the context of armed conflicts[18], and it is the cyber weapons that present a specific interest for our discussion. In this perspective, it is interesting to address the strategic actions of different states in the field of cyber defense. The analysis shows that there are two common approaches to regulating military dimension of cyberspace: 1. implementation of a separate strategy for cyber defense[19], 2. covering the military dimension of cyberspace in the framework of cyber security strategy or covering the military dimension of cyberspace in the framework of a more generic document, such as national defense strategy/ development plan[20]. Both approaches have their advantages and drawbacks. Thus, the clear separation of the cyber defense from other military domains and from cyber security allows the state to better analyse the character of cyber threats during armed conflicts, more accurately tailor the needs in cyber defense sector and plan the advancement of cyber defense forces. However, such an approach risks to overlook the interconnectedness of civil and military infrastructures and the interconnectedness between cyber-defense and defense in other domains, as well as the overlapping issues in cyber defense and cyber security. At the same time addressing cyber defense in the framework of cybersecurity or in a more generic military doctrine of the state would most likely result in insufficient attention to the defense aspects of cyber domain, and, consequently, weaker cyber defense. From the analysis of the content of the strategies we could conclude that most states acknowledge cyberspace as a military domain like land, air or maritime, analyse the main specific characteristics of cyber weapons, and set state objectives and action plan for cyber offense, cyber defense and cyber deterrence respectively. While the future quasi-military dimension of the big data management seems to be overlooked in general, being as a rule viewed in the light of standard privacy and data protection-focused international or national legal regulations, maybe justified by the implications that such a scenario is more far distanced from now and less probable.

For the time being, everyone's wish and efforts should be directed towards creating guarantees that the technological development is used for the benefit of mankind, for raising the threshold of our expectations towards the level of humanity rather than erasing the humanness and realness. Otherwise the civilization might end up finding itself in a situation predicted by Einstein: "I know not with what weap-

[17] At the regional level cyber-crime is regulated with the CoE Convention on Cybercrime (Budapest Convention), CETS No.: 185 (Budapest, 2001), while at the universal level there is no binding instrument that would explicitly address cybercrime. Several treaties (e.g. UN Convention against Transnational Organized Crime (Palermo, 2000)) indirectly impose regulations for cybercrime. The relevant international-legal regulations have shaped the legislation of the state-parties in the realm of cyberspace regulation, however such regulation is applicable only to criminal conduct in the cyberspace and not cyber weapons means and their use during an IAC or NIAC.

[18] There is no international treaty explicitly regulating cyber weapons, leaving us with IHL principle on prohibition of inherently indiscriminate weapons as the main relevant regulation.

[19] For instance, Belgium, Czech Republic, Denmark, Netherlands, Portugal, USA, etc. See: The NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/library/strategy-and-governance/ (accessed 28.02.2022).

[20] For instance, Estonia, Iceland, Lithuania, Montenegro, etc. See: The NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/library/strategy-and-governance/ (accessed 28.02.2022).

ons world war III will be fought but world war IV will be fought by sticks and stones".

8. Conclusions

Throughout history our world has several times passed through cardinal changes triggered by drastic scientific or technological development, new discoveries and mindset or thinking transformation for the given time-period. However, the 21-st century evolution is unique, in particular, by the rapidity of the development, by the nature of the actors causing the change, and uncertainty and the inner seeming controversies and unity of the phenomena comprising this change. These changes affect all spheres of life, including military affairs. Wars on the one hand and the on-going globalisation and science-technological development on the other hand are interdependent.

With regard to the current generation of cyber weapons, it could be concluded that even if they might *prima facie* seem to be inherently indiscriminate, cyber weapons are not *per se* indiscriminate, but rather are weapons with a very high potential of being used indiscriminately or in violation of the principle of discrimination. However, the high potential of indiscriminate use of cyber weapons does not outlaw the cyber weapons as such. Thus, we also agree with the widely accepted opinion that the cyber weapons, which are currently used, are sufficiently regulated by the International Law. At the same time, the future tendencies for advancement and improvement of military cyber technologies, inter alia, via integration of artificial intelligence, may seriously call into question the possibility of their application in compliance with the international legal regulations. At the same time, the possible scenarios of advancement of Big Data management have led us to the conclusion that big data management per se has the potential of being used as a weapon with less lethal or even non-lethal consequences, however equally effective in enforcing one's policy as the traditional weapons or potentially kinetic cyber-weapons. If big data analysis at its current stage of development does not produce very accurate predictions, the well-distributed and structured informational flow in the cyber domain is capable of influencing and manipulating behaviours. In such case if Big data monopoly (including both: hardware and software) vests in one or several actor, it could drastically change the nature of war by making the element of violence redundant and consequently alter the geopolitical balance. Eventually, one of the measures for early response to future challenges could be through reflecting on lex ferenda in cyber security and cyber defence national strategies. From the analysis of the content of different strategies it could be concluded that most states acknowledge cyberspace as a military domain like land, air or maritime, analyse the main specific characteristics of current generation of cyber weapons, and set state objectives and action plan for cyber offense, cyber defense and cyber deterrence. While the future advancement of cyber means of warfare and the quasi-military dimension of the big data management remain overlooked by states in general.

References

1. Alford L., Jr. Cyber Warfare: Protecting Military Systems. – *Acquisition Review Quarterly.* 2000. Spring. P. 101-120.
2. Arkin R. Ethical restraint of lethal autonomous robotic systems: Requirements, 33 research, and implications. – *Autonomous Weapon Systems: Technical, Military, Legal And Humanitarian Aspects.* 2014. P. 33-37. URL: https://www.aph.gov.au/DocumentStore.ashx?id=b64a259c-b9ca-4be1-b5ce-a16dde8adda0&subId=303585 (accessed 28.02.2022).
3. Chi M. Big Data in National Security. 2017. 8 p. URL: https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2017-08/SI118%20Big%20data%20in%20national%20security.pdf?VersionId=jC6LVa_KTXFtDr.W_sBfJbXpatWEDeWA (accessed 28.02.2022).
4. Cirenza P. An Evaluation of the Analogy Between Nuclear and Cyber Deterrence. 2015. 134 p. URL: https://stacks.stanford.edu/file/druid:sh530vk4641/An%20Evaluation%20of%20the%20Analogy%20Between%20Nuclear%20and%20Cyber%20Deterrence.pdf. (accessed 28.02.2022).
5. Clausewitz C. *On War.* Princeton: Princeton University Press. 1984. 752 p.
6. *Customary International Humanitarian Law. Vol. 1. Rules.* Ed. by L-M. Henckaerts and L. Doswald-Beck. Cambridge: Cambridge University Press. 2005. 689 p.
7. Danelyan A., Gulyaeva E. International Legal Aspects of Cybersecurity. – *Moscow Journal of International Law.* 2020. No.1. P. 44–53. DOI: https://doi.org/10.24833/0869- 0049-2020-1-44-53
8. Dinstein Y. *The Conduct of Hostilities under the Law of International Armed Conflict*. 2nd ed. Cambridge: Cambridge University Press. 340 p. DOI: https://doi.org/10.1017/CBO9780511845246
9. Hatch B. Defining a Class Of Cyber Weapons As WMD: an Examination Of the Merits. – *Journal of Strategic Security.* 2018. Vol. 11. No.1. P.43-61. DOI: 10.5038/1944-0472.11.1.1657
10. Kaldor M. *New and Old Wars: Organized Violence in a Globalized Era.* 3rd ed. Cambridge: Polity Press. 2012. 268 p.
11. Lye Chee Wei P. The Nature Of War–Unchanging In The Face Of Shifting Forms And Material Dimensions. – *Pointer Journal of the Singapore armed forces.* 2020. Vol.45. No.2. P. 23-30.

12. Pappila O. The Nature of War today. – *Kungl Krigsvetenskapsakademiens Handlingaroch Tidskrift*. 2008. No. 4. P. 69-73.
13. Shackelford S. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. – *Berkeley Journal of International Law*. 2009. Vol. 27. Issue 1. P. 192-250.
14. Talbot Jensen E. Cyber Warfare and Precautions against the Effects of Attacks. – *Texas Law Review*. 2009. Vol. 88. P. 1533-1569.
15. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Ed. by M. Schmitt. Cambridge: Cambridge University Press. 2017.598 p.
16. *Tallinn Manual Applicable to International Law Applicable to Cyber Warfare*. Ed. by M. Schmitt. Cambridge: Cambridge University Press. 2013. 302 p.
17. Yeremyan L., Harutyunyan D, Freedom Of Thought Endangered In The 21st Century? Legal Protection from Manipulation. – *Wisdom*. 2020. Vol. 14. Issue 1. P. 131-147.

About the Authors

Ara Yeremyan,
Cand. Sci. (Law), Associate Professor, Russian-Armenian University

123, Hovsep Emin, Yerevan, Republic of Armenia, 0051

ara_yeremian@yahoo.com
ORCID: 0000-0001-9494-9943

Lilit Yeremyan,
Cand. Sci. (Law), Associate Professor, Russian-Armenian University

123, Hovsep Emin, Yerevan, Republic of Armenia, 0033

lilityer@gmail.com
ORCID: 0000-0002-5127-3776

Информация об авторах

Ара Владимирович Еремян,
кандидат юридических наук, доцент, Российско-Армянский Университет

0051, Республика Армения, Ереван, ул. Овсепа Эмина, д. 123

ara_yeremian@yahoo.com
ORCID: 0000-0001-9494-9943

Лилит Араевна Еремян,
кандидат юридических наук, доцент, Российско-Армянский Университет

0033, Республика Армения, Ереван, ул. Овсепа Эмина, д. 123

lilityer@gmail.com
ORCID: 0000-0002-5127-3776