




DOI: 10.22363/2313-0660-2025-25-1-67-77

EDN: KACFAB

Research article / Научная статья

## The Principle of Distinction Between Civilian Objects and Military Objectives in the Context of the Development of Information and Communication Technologies in Armed Conflicts

Yao N. Adu<sup>1,2,3</sup>  , Mirzet S. Ramich<sup>1</sup> <sup>1</sup>RUDN University, Moscow, Russian Federation<sup>2</sup>Orenburg State University, Orenburg, Russian Federation<sup>3</sup>Ural State University of Economics, Ekaterinburg, Russian Federationadu-ya@rudn.ru

**Abstract.** The destruction of infrastructure in modern armed conflicts, whether civilian or military, has led to renewed of interest in the discussion on the distinction between civilian objects and military objectives in the current international instruments of international humanitarian law (IHL). On the one hand, in contemporary realities, the presence of heavy artillery is not an advantage without modern information and communication technologies (ICT), which determine the benefits of the parties to the conflict, in particular in the context of the concept of network-centric warfare, which implies a unified system of troop control, the effective use of satellites to identify the dislocation of enemy troops, etc. On the other hand, the information space has become a full-fledged battlefield, where information and cyber operations are conducted to reduce the enemy's morale, create social tension, and paralyze the operation of critical information resources. The availability of advanced communication systems, the Internet, and satellite data is an undoubted advantage in modern warfare, which complicates the concepts of distinction between civilian objects and military objectives, especially when the same object can serve both civilian and military purposes. The purpose of this article is to analyze the complexities that have arisen in the definition of a civilian object in the context of the development of ICTs due to their dual use for both civilian and military purposes in relation to modern conflicts. As a result of the study, the authors conclude that the definitions of civilian objects, as outlined in IHL, become more complex in the context of the development of ICT given its dual purpose. The authors assume that despite the protective measures afforded by contemporary international law with regard to civilian objects, the development of ICTs “erodes” the criteria for their definition in modern armed conflicts.

**Key words:** international humanitarian law, integrated infrastructure of information and communication technologies, dual-use facilities, Geneva Conventions of 1949

**Conflicts of interest.** The authors declare no conflicts of interest.

**Authors' contributions.** The authors made an equal contribution to the design, research and preparation of the final article's text.

**For citation:** Adu, Y. N., & Ramich, M. S. (2025). The principle of distinction between civilian objects and military objectives in the context of the development of information and communication technologies in armed conflicts. *Vestnik RUDN. International Relations*, 25(1), 67–77. <https://doi.org/10.22363/2313-0660-2025-25-1-67-77>

---

© Adu Y.N., Ramich M.S., 2025



This work is licensed under a Creative Commons Attribution 4.0 International License

<https://creativecommons.org/licenses/by-nc/4.0/legalcode>

## Разграничение гражданских и военных объектов в условиях развития информационно-коммуникационных технологий в ходе вооруженных конфликтов

Я.Н. Аду<sup>1,2,3</sup> , М.С. Рамич<sup>1</sup> 

<sup>1</sup>Российский университет дружбы народов, Москва, Российская Федерация

<sup>2</sup>Оренбургский государственный университет, Оренбург, Российская Федерация

<sup>3</sup>Уральский государственный экономический университет, Екатеринбург, Российская Федерация

✉ adu-ya@rudn.ru

**Аннотация.** Поражение разных объектов как гражданского, так и военного назначения в современных вооруженных конфликтах реанимирует дискуссию о разграничении гражданских и военных объектов в действующих международных инструментах в международном гуманитарном праве (МГП). В современных реалиях, с одной стороны, наличие тяжелой артиллерии не является преимуществом без современных информационно-коммуникационных технологий (ИКТ), которые могут обеспечить превосходство одной из сторон конфликта, в частности в контексте концепции сетецентричных войн, подразумевающих единую систему управления войсками, эффективное использование спутников для выявления дислокации войск противника и т. д. С другой стороны, информационное пространство стало полноценным театром военных действий, где проводятся информационные и кибероперации, направленные на снижение боевого духа противника, создание социальной напряженности и парализацию работы критически важных информационных ресурсов. Наличие продвинутых систем связи, Интернета и спутниковых данных является безусловным преимуществом в современных конфликтах, но осложняет разграничение характеристик гражданского и военного объекта, особенно в условиях, когда один и тот же объект может служить для гражданских и военных целей. Цель исследования — проанализировать трудности, возникшие в определении гражданского объекта в контексте развития информационно-коммуникационных технологий в связи с их двойным использованием как в гражданских, так и в военных целях применительно к современным конфликтам. Авторы приходят к выводу, что определение гражданского объекта, как представляется в МГП, усложняется в условиях развития информационно-телекоммуникационных технологий ввиду своего двойного назначения. Несмотря на то, что современные положения международного права защищают гражданские объекты, развитие ИКТ «размывает» критерии их определения в условиях современных вооруженных конфликтов.

**Ключевые слова:** международное гуманитарное право, комплексная инфраструктура информационно-коммуникационных технологий, объекты двойного назначения, Женевские конвенции 1949 года

**Заявление о конфликте интересов.** Авторы заявляют об отсутствии конфликта интересов.

**Вклад авторов.** Авторы внесли равнозначный вклад в разработку дизайна, проведение исследования и подготовку текста статьи.

**Для цитирования:** Аду Я. Н., Рамич М. С. Разграничение гражданских и военных объектов в условиях развития информационно-коммуникационных технологий в ходе вооруженных конфликтов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2025. Т. 25, № 1. С. 67–77. <https://doi.org/10.22363/2313-0660-2025-25-1-67-77>

### Introduction

The question of the distinction between civilian objects and military objectives has been the subject of debate among scholars since the adoption of the four Geneva Conventions of 1949 and their Additional Protocols due to the fact that these instruments do not provide a clear definition of these objects. The content of Article 52 of Additional Protocol I defines abstractly or incompletely what civilian objects

and military objectives are. The issue of the legal status of a civilian object, especially one with a dual purpose, remains the subject of consideration and analysis by Russian and foreign scholars.<sup>1</sup>

<sup>1</sup> See: Tiunov O. I. International Humanitarian Law: Textbook. Moscow: Izd-vo Norma publ., 2023. (In Russian); International Law: in 2 volumes. Vol. 2: Special Part: Textbook for Universities. 2nd edition / ed. by A. Y. Kapustin. Moscow: Izd-vo Yurait publ., 2025. (In Russian). See also: (Furcalo, 1982; Blishchenko, 1984;

The definition of a civilian object is complicated by the use of modern information and communications technology (ICT) that present complex civil and military inventions and infrastructures for a variety of purposes (both military and civilian).

The purpose of this article is to identify the consequences of the lack of a clear definition of the civilian object in the instruments of international humanitarian law and the difficulties encountered in attempting to address this issue, particularly in the field of ICT. To this end, the following complex tasks must be completed: to define the concept of civilian objects and its legal significance in international humanitarian law (IHL), to analyze the complexity of the distinction between civilian objects and military objectives, especially in the context of the development of ICT due to their dual purpose, including both civilian and military purposes, and to determine the responsibility of belligerents in the conditions of warfare.

### ICTs in Modern Armed Conflicts

Given the complexity of its legal scope, there are several definitions. Currently, the most common definition of international humanitarian law, which is used in Russian academic literature, belongs to the Russian scholar O.I. Tiunov. According to him, “International humanitarian law is a branch of international (public. — *Authors’ note.*) law, consisting of a set of international legal principles and norms applicable in armed conflicts (international and non-international), providing for the rights and obligations of actors of international law and other parties to armed conflicts to respect and ensure the protection of victims of armed conflicts, civilians, civilian objects and cultural property, as well as their obligations to protect victims of armed

conflicts, civilian population, civilian objects and cultural property.”<sup>2</sup>

The sources of international humanitarian law consist mainly of the so-called Hague Law, Geneva Law and other international legal norms adopted in this field. The development and adoption of The Hague and Geneva Law have their roots in the second half of the 18th and early 19th centuries, when modern ICTs did not yet exist or were only at the beginning of their development and evolution.

Nowadays, almost half a century passed after the adoption of three Additional Protocols<sup>3</sup> to the four Geneva Conventions,<sup>4</sup> there has been a great leap of development in the field of ICT, unprecedented in the history of the development of human society. While serious progress has been made in recent decades in the area of means of warfare, for example, in prohibiting of the production, stockpiling and proliferation of certain weapons, such as biological,<sup>5</sup> bacteriological,<sup>6</sup> nuclear,<sup>7</sup> etc., others, such as hypersonic or laser weapons, are partially or completely unregulated by contemporary international humanitarian law. The same can be said of ICTs, which have become an important part of the military capabilities of a number of states.

<sup>2</sup> International Law : in 2 volumes. Vol. 2: Special Part : Textbook for Universities. 2nd edition / ed. by A. Y. Kapustin. Moscow: Izd-vo Yurait publ., 2025. P. 102. (In Russian).

<sup>3</sup> Geneva Conventions of 1949, Additional Protocols and Their Commentaries // International Humanitarian Law Databases. URL: <https://ihl-databases.icrc.org/en/ihl-treaties/geneva-conventions-1949additional-protocols-and-their-commentaries> (accessed: 30.11.2022).

<sup>4</sup> Ibid.

<sup>5</sup> Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction // The United Nations. (In Russian). URL: [https://www.un.org/ru/documents/decl\\_conv/conventions/bacweap.shtml](https://www.un.org/ru/documents/decl_conv/conventions/bacweap.shtml) (accessed: 30.11.2022).

<sup>6</sup> Ibid.

<sup>7</sup> Treaty on the Prohibition of Nuclear Weapons // The United Nations. July 7, 2017. (In Russian). URL: <https://docs.un.org/ru/A/CONF.229/2017/8> (accessed: 30.11.2022).

Smith, 2002; Schmitt, 2008; Dinstein, 2012; Liivoja & McCormack, 2016).

J.S. Nye, compared the development of cyber capabilities of countries with nuclear weapons, hypothesizes that attacks from cyberspace, where costs are relatively low, can be directed against targets in the real world, where resources are limited and costly (Nye, 2011, p. 19). At the same time, *fourth-generation warfare* theory suggests that all possible ‘networks’ should be used to convince political decision makers on the adversary’s side that their political goals are unattainable or unreasonably costly to achieve, this combines physical and virtual attacks to achieve their goals (Betz & Stevens, 2011).

Even in the distant past people could understand the importance of information (Jayan, 2009, p. 1) and the possibility of its transmission even with limited means, but today the rapid development of ICTs has had a profound impact on all spheres of life. In exploring the role of ICTs in the development of modern weapons in the warfare strategy of states, Thomas W. Smith (2002) even divides countries into hi-tech states and low-tech countries. It is also true that there is a hierarchical division of countries according to their ability to influence in the information sphere into those who determine the rules (*rule-maker*) and those who adopt these rules due to the lack of proper technological capacity (*rule-taker*) (Ramich & Piskunov, 2022).

Moreover, the objects employed in information-psychological operations, whose task is to exert the greatest influence on society and decision-makers through information resources, deserve special attention. On the one hand, the counteraction against disinformation and fakes is possible in the information space with the help of blocking and content filtering tools and, on the other hand, due to the large size of the information space, physical destruction of the source of the threat in the network may be a less costly and more effective solution to the problem. Thus, according to the Russian media, on February 24, 2022, one of the first facilities targeted on the territory of

Ukraine was the headquarters of the 72nd Center for Information and Psychological Operations of the Armed Forces of Ukraine.<sup>8</sup> On the one hand, this confirms the importance of information-psychological operations in modern conflicts, and on the other hand, it updates the issue of classification from the point of international law view of the objects used for information-psychological operations, especially in the context of the possible location of these objects not on the territory of the countries participating in the conflict and the possibility of engaging private contractors.

Thus, this study focuses on the use of information and communication technologies as a means of conducting warfare and their compatibility with the concept of ‘civilian object’ in contemporary armed conflicts.

The use of satellite data by the parties to the armed conflict and, in particular, by Ukraine through civilian satellite stations (*Starlink*) and other satellite data provided by third countries (North Atlantic Treaty Organization (NATO) and the USA) raises the question of the distinction between the concepts of civilian objects and military ICT infrastructures. In fact, the practice and tactics of using ICTs are not new methods of warfare.

It should be recalled that current international instruments in the field of IHL do not fully define what constitutes a ‘civilian object.’<sup>9</sup> Usually a civilian object is presented as something other than a ‘military object.’

<sup>8</sup> Alshaeva I. “To Avoid Brainwashing”: The Headquarters of the “Troll Factory” of the AFU Was Liquidated // *Gazeta.ru*. February 25, 2022. (In Russian). URL: <https://www.gazeta.ru/army/2022/02/25/14577799.shtml> (accessed: 24.06.2023).

<sup>9</sup> See: International Law : in 2 volumes. Vol. 2: Special Part : Textbook for Universities. 2nd edition / ed. by A. Y. Kapustin. Moscow: Izd-vo Yurait publ., 2025. (In Russian); Sassoli M. Legitimate Purposes of Attack in International Humanitarian Law // International Committee of the Red Cross. January 23, 2004. (In Russian). URL: <https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm> (accessed: 15.05.2023).

Article 52 of Protocol I Additional to the Geneva Conventions of 1949 relating to the Protection of Victims of International Armed Conflicts (hereinafter Protocol I) defines that “civilian objects are all those objects which are not military objectives.”<sup>10</sup> The second paragraph of the same article defines a military objective as follows: “Military objective shall be limited to those objects which, by their nature, location, purpose or use, make an effective contribution to military action and the total or partial destruction, capture or neutralization of which, under the circumstances existing at the time, confers a distinct military advantage.”<sup>11</sup> The very definition of ‘military objective’ is not specific, as the phrase “A military objective, by virtue of its nature ... provides a distinct military advantage” in modern contexts requires serious clarification.

Thus, the wording of Article 52, paragraph 2, of the Protocol, as M. Sassoli notes, is abstract<sup>12</sup> and allows for a wide interpretation by different parties. Therefore, Thomas W. Smith, in his analysis of the current norms of IHL, believes that IHL contributes to the development of armaments (Smith, 2002, p. 362).

However, based on this definition, certain characteristics of a military installations can be noted regarding its nature, location and purpose. These characteristics should give a clear military advantage to both the defending country and the enemy when defeated. The definitions of ‘civilian object’ and ‘military

objectives’ from Protocol I seem to lead to a wide interpretation, including among scholars and specialists.

Thus, some authors try to provide their own definition, which could serve as an example in the future when drafting and adopting new international legal rules in the field of IHL or when amending existing instruments. For instance, according to Yu.V. Puzyreva, “Military objectives can be both objects specially designed for military use (military equipment, ammunition factories, warehouses of military equipment, etc.) and civilian objects (an apartment building or a bridge become military objectives due to their tactical use by the defending party) (Puzyreva, 2006).

Thus, it is fair, from our point of view, Yu.V. Puzyreva’s remark that *there are no objects or objectives that are exclusively civilian or military, since civilian objects*, such as residential buildings, bridges, railroad tracks, satellite stations, power supply stations, etc., due to their tactical use by the defending party can be considered military objectives and, accordingly, military lawful targets, confirmation of which can be seen at present in Ukraine.

For example, the non-governmental organization Amnesty International noted in a statement on August 4, 2022, that Ukraine deploys military equipment in settlements, schools and hospitals.<sup>13</sup> In such a case, said civil objects become legitimate targets.

It should be noted that IHL establishes the same rules, rights and obligations for parties to a conflict, without distinguishing between offensive and defensive operations. Recall that during Operation “Desert Storm” in 1990–1991 in Iraq more than half of the list of 12 objectives approved by the coalition countries included

<sup>10</sup> Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 // Electronic Fund of Legal and Normative-Technical Documents. (In Russian). URL: <https://docs.cntd.ru/document/901755843> (accessed: 15.05.2023).

<sup>11</sup> Ibid.

<sup>12</sup> Sassoli M. Legitimate Purposes of Attack in International Humanitarian Law // International Committee of the Red Cross. January 23, 2004. (In Russian). URL: <https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm> (accessed: 15.05.2023).

<sup>13</sup> Ukraine: Military Endangering Civilians by Locating Forces in Residential Areas — New Research // Amnesty International. August 4, 2022. URL: <https://www.amnesty.org.uk/press-releases/ukraine-military-endangering-civilians-locating-forces-residential-areas-new> (accessed: 15.05.2023).

civilian objects: power supply, telecommunications, bridges, water reservoirs, etc. (Smith, 2002, p. 364). Similar tactics of destroying civilian infrastructure and dual-use facilities were also used in the Yugoslavia by NATO countries (Boothby, 2018, p. 7).

Thus, a clear definition of the civil object is especially relevant in the context of globalization and the rapid development of ICTs. Everything that was previously used in ICTs inclusively for military purposes is now in the public domain, that is, the civilian domain. All this complicates the determination of their legal status during wartime.

William H. Boothby (2018, p. 7) rightly points out that the development of radar systems during World War II and their use in civil aviation contributed to safety in this area. That's what the dual use of military facilities for civilian purposes and vice versa is all about. The situation is similar with satellite navigation systems. Initially, the US *Global Positional System* (GPS) and the Russian Global Navigation Satellite System (*GLONASS*) had exclusively military purposes. For example, back in the 1990–1991 in Iraq, the Pentagon used GPS technology in airstrikes to make them more accurate (Smith, 2002, p. 366), as well as in guiding precision-guided missiles. However, while such satellite navigation systems, on the one hand, have been used for military purposes, on the other hand, they are now already widely used for civilian purposes. However, their original purpose has not been exhausted, and they do not only make an invaluable contribution to the development of civilian ICTs, but also provide a significant military advantage in warfare by the parties, as they do not only provide real-time geo-positions of the enemy, but can also be used to control aircraft.

### **The Dilemma of Civilian ICT Infrastructure in Armed Conflict**

The deployment of ICT infrastructure and its dual use raises serious questions when

defining a civilian facility. The issue arises as to whether a civilian '*information and telecommunications technology infrastructure complex*' deployed on residential buildings or in residential neighborhoods can be hit, if the defending party has not removed it from these locations and at the same time uses it for military purposes and this gives it a clear military advantage. Generally, these are satellite dishes and other broadcasting facilities, but they also include other infrastructures that support their operation, such as power generation facilities and other stations. Under the current Geneva Conventions, such infrastructures, along with other civilian objects, will be protected, only if there is doubt about their use for military purposes by the defending party. However, despite their location among civilian targets, they can become military targets under Protocol I, as happened during military operations in Iraq and in Yugoslavia.<sup>14</sup>

Obviously, the drafters of the Geneva Conventions and related Protocols could not have foreseen this and cannot at present determine how information and communication technologies will develop in the coming years. This is a major challenge for contemporary IHL, and the term we use, '*complex information and communications technology infrastructure*,' is also of great significance. The 'complex infrastructure of information and communication technologies' along with other equipment serving this sphere of activity should be understood as power complexes, antennas, towers (television, telecommunication), communication routes that provide access to this infrastructure or support its uninterrupted functioning, etc. The complex ICT infrastructure, as practice shows, is a critical infrastructure of the state, vital for the normal functioning of the economy and other

<sup>14</sup> Sassoli M. Legitimate Purposes of Attack in International Humanitarian Law // International Committee of the Red Cross. January 23, 2004. (In Russian). URL: <https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm> (accessed: 15.05.2023).

spheres of activity of the country (Gallais & Filiol, 2017). An integrated ICT infrastructure inevitably becomes a legitimate military objective under Article 52 if it can be shown that it is used by the defending party because it provides it with a military advantage.

To adapt to the changing environment, NATO has developed the Tallinn Manual on International Law Applicable to Cyber Operations, which articulates key concepts and approaches to the new challenges and threats posed by digitalization. This paper devotes several sections to the topic of distinguishing between civilian and military ICT facilities. In particular, Rule 100 states that ICT infrastructure objects may be recognized as military objectives if they meet one of four criteria: essence, location, purpose, and use.<sup>15</sup>

Firstly, the Tallinn Manual differentiates between the concepts of military purpose in the legal and operational sense, e.g. an operational purpose could be to neutralize the transmission of electronic communications; the communications themselves would not be a legal military purpose in the legal sense, but the equipment used to receive and transmit such communications would be considered as such.<sup>16</sup>

Secondly, computers and other ICT infrastructure are defined as military objectives based on the criterion of “nature,” is important in the context of military command, control, communications, computers, intelligence, tracking and reconnaissance. In terms of the provisions of the Tallinn Manual, “Military information systems, wherever located and the facilities in which they are permanently located, qualify as military installations. The fact that civilians (government employees or contractors) may operate these systems is irrelevant to the

question of whether they qualify as military installations.”<sup>17</sup>

There is also a need to ensure that civilian objects are not used for military purposes, and third, when civilian objects are used for military purposes, they are reclassified as military objectives. Thus, “If a party to a conflict uses a particular civilian computer network for military purposes, that network loses its civilian character and becomes a military objective. This is true even if the network also continues to be used for civilian purposes.”<sup>18</sup> Also, an enterprise producing computer equipment under contract with the enemy armed forces will be considered a military facility, even if the same enterprise produces civilian goods.<sup>19</sup>

Fourth, an object may be recognized as military under the criteria of “location,” which may give one party a military advantage, or “purpose,” which allows the object to be used for military purposes in the future.<sup>20</sup>

There are several examples where civilian facilities have been reclassified as military because of meeting the criteria.

The first example relates to Operation Allied Force 1999. NATO justified the bombing of the TV tower in Belgrade during the operation in the former Yugoslavia to military necessity, arguing that television was a propaganda tool of the country’s authorities<sup>21</sup> and thus justifiably a military target.

The second example is related to the conflict in Ukraine. In Russian Federation on October 8, 2022, there was an explosion on the Crimean Bridge, which led to its partial collapse. The results of the investigation

<sup>17</sup> Ibid. P. 438.

<sup>18</sup> Ibid. P. 438–439.

<sup>19</sup> Ibid.

<sup>20</sup> Ibid. P. 439–440.

<sup>21</sup> Sassoli M. Legitimate Purposes of Attack in International Humanitarian Law // International Committee of the Red Cross. January 23, 2004. (In Russian). URL: <https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm> (accessed: 15.05.2023). See also: (Smith, 2002, p. 366).

<sup>15</sup> Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge : Cambridge University Press, 2017. P. 435–445.

<sup>16</sup> Ibid. P. 436.

conducted by the Russian special services confirmed the Ukrainian fact in this incident,<sup>22</sup> although officially the country's leadership, represented by Ukrainian President V.A. Zelenskyy, denied Kiev's involvement in this explosion.<sup>23</sup> Commenting on this incident on Western TV channels (especially French ones), many experts considered the Crimean Bridge to be a legitimate military target for Ukraine, i.e. it was equated to military objectives, as it provided a military advantage to Russia,<sup>24</sup> despite the fact that the Crimean Bridge is the only connecting artery between the Russian part of the mainland with the peninsula. They claim that Russian troops use this route to supply military units during the special military operation (SMO).<sup>25</sup>

It is worth noting that the explosion on the Crimean bridge changed the way the SMO was conducted, as the Russian Army began striking important energy infrastructure facilities in Ukraine, although prior to the incident, strikes were carried out exclusively on military infrastructure, according to the Russian military leadership.<sup>26</sup> According to Article 52 of Protocol 1, strikes against Ukrainian strategic infrastructure facilities are also a military necessity, i.e. legally justified objectives, since "*the same complex infrastructure*" is used by

Ukraine for strikes against Russian troops and on the territory of the Russian Federation.

This could also include the U.S. transfer of satellite communication stations (*Starlink*) to Ukraine, giving it with a military advantage, as *Starlink* is also used not only for communication, but also for controlling unmanned aerial vehicles (UAVs),<sup>27</sup> for data collection, etc. during military operations. Accordingly, Ukraine's 'complex strategic information and communications technology infrastructure' becomes an obvious legitimate target for Russian forces: power supply, satellite dishes, railroad tracks, etc., which form and provide the complexity of Ukraine's information and communications technology infrastructure, as they contribute greatly "to the enemy's ability to fight or support the war effort," as D.S. Malikov (2014, p. 166) writes. The author also rightly notes that certain countries, when choosing a target, will take into account the military advantage expected from the attack as a whole, rather than from its individual parts (Malikov, 2014, p. 166). In addition, according to Article 52, paragraph 2, an important place among the attributes of a military objective is its location.

However, given the complexity of the ICT infrastructure, it can be seen in this case that even ordinary satellite dishes located on private houses in populated areas become legitimate military targets in the conducting of warfare in modern realities, as they provide a military advantage to the enemy. NATO's actions in Iraq and Yugoslavia are evidence of this.

Consequently, the question arises as to how to fill the gap in the norms of IHL, taking into account the current realities of the development of ICTs. From our perspective, the development of ICTs will only aggravate the situation related to the problem of civilian objects and military

<sup>22</sup> FSB Published Materials on How the Explosion on the Crimean Bridge Was Prepared // RIA Novosti. October 12, 2022. (In Russian). URL: <https://ria.ru/20221012/most-1823287523.html> (accessed: 15.05.2023).

<sup>23</sup> Polyakova V. Zelensky Said That Kiev Did Not Order the Terrorist Attack on the Crimean Bridge // RBC. October 20, 2022. (In Russian). URL: <https://www.rbc.ru/politics/20/10/2022/63513b7b9a7947798da528f5> (accessed: 15.05.2023).

<sup>24</sup> Sauvage G. L'attaque du pont de Crimée, point culminant des revers russes en Ukraine // France24. 12.10.2022. URL: <https://www.france24.com/fr/europe/20221009-guerre-en-ukraine-le-pont-de-crim%C3%A9e-touch%C3%A9-la-russie-accumule-les-revers> (accessed: 19.01.2023).

<sup>25</sup> Ibid.

<sup>26</sup> Briefings // Ministry of Defence of the Russian Federation. (In Russian). URL: [https://z.mil.ru/spec\\_mil\\_oper/brief/briefings.htm](https://z.mil.ru/spec_mil_oper/brief/briefings.htm) (accessed: 01.11.2022).

<sup>27</sup> Elon Musk Refused to Supply Ukraine with Satellite Internet for Free // CNews. October 14, 2022. (In Russian). URL: [https://www.cnews.ru/news/top/2022-10-14\\_ilon\\_mask\\_otkazalsya\\_besplatno](https://www.cnews.ru/news/top/2022-10-14_ilon_mask_otkazalsya_besplatno) (accessed: 29.11.2022).



objectives distinction, as the analysis of some modern means and methods of warfare shows. The classical ways of conducting war, on which the norms of the Geneva Conventions and their Protocols were based, have already fallen behind the times.<sup>28</sup> Today, not only conventional weapons (e.g., artillery), but also drones, unmanned aerial vehicles, etc., which use information and communication technologies to transmit data, play a key role in warfare tactics. In such conditions, an ordinary engineer working for a private company assembling sensors, drones, or even a simple IT specialist, can provide a significant advantage during a conflict that was not previously envisioned by the drafters of the various Geneva Conventions.

Rightly notes M. Sassoli, referring to the comments on the German Military Regulations, concerning the attack on the civilian population: “If the intention to have a direct effect on the determination of the people of the enemy side to fight were recognized as a legitimate purpose of the use of military force, there would be no limitations left in warfare.”<sup>29</sup> Also, given that the ultimate goal of the IHL, by F.F. Martens (Kukushkina, Joirysh & Shishkin, 2019, p. 160), is aimed at mitigating and minimizing the consequences of military actions on the civilian population of the conflicting parties, we believe that it is necessary to supplement Article 52 of Additional Protocol I, by exempting civilian objects from military purposes, including ICT objects, even if they are dual-use, especially when located in populated areas, since expert commentaries to the articles of the Geneva Conventions do not establish an obligation for the country parties to the Geneva Conventions. In this regard, warring parties’ responsibility for attacking or using dual-use ICTs or civilian

dual-use facilities for military purposes should be strengthened if they are predominantly used for civilian purposes as part of the ICT infrastructure. A similar approach already exists in IHL, where strikes against nuclear or other dangerous sources (e.g., hydropower plants, nuclear power plants, dams) are prohibited despite their purpose (military facilities or not) and location, i.e., proximity/distance to populated areas (Boothby, 2018, p. 52), thus saving civilian lives in times of war. We believe that a similar interpretation can also be applied to ICTs.

Also, as M. Sassoli pointed out, a list should be maintained that clearly defines civilian objects as military objectives, with the possibility of modification to take into account the development of modern ICTs or international relations in general.

Another important aspect is the possibility of using ICTs to inflict damage on a state without actually starting hostilities, which could be a cyberattack on critical infrastructure or objects significant to social or state life. The main issue is the definition of the “threshold” that can be considered permissible for a cyberattack to be considered a violation of sovereignty with all the consequences under international humanitarian law.

A possible solution for the present stage of development of international norms in the ICT sphere may be ‘soft regulation,’ which allows to define norms and rules of conduct by multilateral organizations in advance and to further lay down these norms in the draft international legal documents by the United Nations. A similar situation has developed around the adoption of an international convention in the field of information security, where there are two approaches: the Russian approach, which implies respect for the inviolability of sovereignty in the fight against the criminal use of ICTs, and the Western approach, which implies “the possibility of combating cybercrime without taking into account state sovereignty and, in fact, implies the

<sup>28</sup> Sassoli M. Legitimate Purposes of Attack in International Humanitarian Law // International Committee of the Red Cross. January 23, 2004. (In Russian). URL: <https://web.archive.org/web/20221011205642/https://www.icrc.org/ru/doc/resources/documents/misc/ihl-attacks-230104.htm> (accessed: 15.05.2023).

<sup>29</sup> Ibid.

extraterritorial extension of the right of the strong in this area.”<sup>30</sup> Respectively, the norms proposed by Russia also formed the basis of the Concept of the UN Convention on Ensuring International Information Security and the documents adopted by the Shanghai Cooperation Organization (SCO) and BRICS, while the norms proposed by Western countries are supported by the United States and adopted by NATO and the European Union.

### Conclusion

In conclusion, the problem of distinguishing between civilian objects and military objectives is very relevant. This distinction is becoming more and more blurred every day, especially with the development of modern ICTs. Our analysis demonstrates that Western countries, in particular NATO member states, in their practice consider civilian dual-use objects to be military objectives, as it was

shown during different military campaigns in Iraq, Kosovo and others. Thus, ICTs undoubtedly offer great prospects in different areas of human life. However, by and large, their primary purpose in the military sphere still remains high, despite their wide introduction into civilian circulation, which will further complicate not only the differentiation of the concept of civilian objects and military objectives, but also the establishment of the responsibility of warring parties for violations of international humanitarian law.

Most ICT infrastructure is dual-use, making it difficult to categorize it as civilian objects or military targets. In addition, the possibility of remote access and cyberattacks from “third countries” raises the question of legitimate countermeasures and the “threshold” of damage required for a response.

The complexity of adopting new international norms and rules is also related to the different approaches of countries to understanding cyberspace and sovereignty in cyberspace, which causes clustering of states with different views and the formation of normative documents on the basis of regional international organizations.

<sup>30</sup> Zinovieva E. S. International Information Security in US-Russian Bilateral Relations // Russian International Affairs Council. March 1, 2023. URL: <https://russiancouncil.ru/en/analytcs-and-comments/analytcs/international-information-security-in-us-russian-bilateral-relations/> (accessed: 26.06.2023).

Received / Поступила в редакцию: 18.10.2023

Revised / Доработана после рецензирования: 04.11.2024

Accepted / Принята к публикации: 24.12.2024

### References

- Betz, D. J., & Stevens, T. (2011). *Cyberspace and the state: Toward a strategy for cyber-power*. Abingdon: Routledge. Retrieved from [https://www.researchgate.net/publication/345705816\\_Cyberspace\\_and\\_the\\_State\\_Toward\\_a\\_Strategy\\_for\\_Cyber-power](https://www.researchgate.net/publication/345705816_Cyberspace_and_the_State_Toward_a_Strategy_for_Cyber-power)
- Blishchenko, I. P. (1984). *Conventional weapons and international law*. Moscow: Mezhdunarodnye otnosheniya publ. (In Russian).
- Boothby, W. H. (2018). *New technologies and the law in war and peace*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781108609388>
- Dinstein, Y. (2012). The principle of distinction and cyber war in international armed conflicts. *Journal of Conflict and Security Law*, 17(2), 261–277. <https://doi.org/10.1093/jcsl/kr015>
- Furkalo, V. V. (1982). *International legal protection of the civilian population during armed conflicts* [dissertation]. Kiev. (In Russian).
- Gallais, C., & Filiol, E. (2017). Critical infrastructure: Where do we stand today? A comprehensive and comparative study of the definitions of a critical infrastructure. *Journal of Information Warfare*, 16(1), 64–87. Retrieved from <https://www.jstor.org/stable/26502877>
- Jayan, S. D. (2009). About information, information technology, cryptography and law. *Journal of the Indian Law Institute*, 51, 1–11. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1804899#](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1804899#)

- Kukushkina, A. V., Joirysh, A. I., & Shishkin, V. N. (2019). International humanitarian law and Martens' clausula. *Zakon i Pravo*, (9), 159–163. (In Russian). <https://doi.org/10.24411/2073-3313-2019-10431>; EDN: URLACB
- Liivoja, R., & McCormack, T. (Eds.). (2016). *Routledge handbook of the law of armed conflict*. London: Routledge. <https://doi.org/10.4324/9780203798362>
- Malikov, D. S. (2014). The definition of the notions of the military and civilian objects in the area of the armed conflict, and the legal assessment of the differences between them. *Vlast'*, (8), 163–168. (In Russian). EDN: SJXJHX
- Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly*, 5(4), 18–38. Retrieved from <https://www.jstor.org/stable/26270536>
- Puzyreva, Yu. V. (2006). Distinguishing between civilian and military objects in international humanitarian law. *Yurist-mezhdunarodnik*, (4), 19–28. (In Russian). EDN: UWCVMH
- Ramich, M. S. & Piskunov, D. A. (2022). The securitization of cyberspace: From rulemaking to establishing legal regimes. *Vestnik RUDN. International Relations*, 22(2), 238–255. <https://doi.org/10.22363/2313-0660-2022-22-2-238-255>; EDN: KSSXFK
- Schmitt, M. N. (2008). The principle of distinction and weapon systems on the contemporary battlefield. *Connections*, 7(1), 46–56. <https://doi.org/10.11610/Connections.07.1.03>
- Smith, T. W. (2002). The new law of war: Legitimizing hi-tech and infrastructural violence. *International Studies Quarterly*, 46(3), 355–374. <https://doi.org/10.1111/1468-2478.00237>

#### About the authors:

*Adu Yao Nikez* — PhD (Law), Associate Professor, Department of Theory and History of International Relations, RUDN University; Associate Professor, Department of State and Law Theory and Constitutional Law, Orenburg State University; Honorary Professor, Ural State University of Economics; eLibrary SPIN-code: 6740-9517; ORCID: 0000-0001-8696-0181; e-mail: [adu-ya@rudn.ru](mailto:adu-ya@rudn.ru)

*Ramich Mirzet Safetovich* — Assistant, Department of Theory and History of International Relations, RUDN University; Researcher, Centre for Applied Analysis of International Transformations, RUDN University; eLibrary SPIN-code: 1830-1087; ORCID: 0000-0003-1479-2785; e-mail: [ramich\\_ms@pfur.ru](mailto:ramich_ms@pfur.ru)