Vestnik RUDN. International Relations. ISSN 2313-0660 (Print), ISSN 2313-0679 (Online) 2026 Vol. 26 No. 1 62–76
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2026-26-1-62-76
EDN: TCJXVU

Review article / Обзорная статья

The Applicability of International Humanitarian Law to Cyber Operations: A Review of Russian and Western Approaches

Vadim B. Kozyulin

Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Moscow, Russian Federation
✉ v.kozyulin@dipacademy.ru

Abstract. The relevance of this study stems from the fact that cyber operations have become an integral element of contemporary armed conflicts, while the applicability of international humanitarian law (IHL) to the digital environment remains contested and is only partially regulated. In practice, this is reflected by the lack of well-established criteria for classifying specific cyber operations as an "attack," a "use of force," or as unfriendly yet formally lawful conduct. Given the transboundary nature of information and communication technologies, the anonymity of actors, and the involvement of non-state entities, there is still no common approach to qualifying cyber activities or protecting civilian infrastructure, which complicates the development of a coordinated international response to cyber incidents. The problem is further exacerbated by the fact that many cyber operations do not cause physical destruction, but rather result in a loss of functionality of systems, calling into question traditional understandings of violence and harm under IHL. The methodology of the study combines a comparative legal analysis of official national positions, United Nations documents, and specialized doctrinal sources, with a systematic interpretation of IHL norms as applied to new forms of armed confrontation. The research employs doctrinal legal analysis, content analysis of governmental doctrines and expert commentaries, as well as elements of case studies focusing on representative cyber incidents, including operations targeting critical infrastructure and dual-use information systems. This article contributes to the literature by providing an integrated examination of three pivotal dimensions of the application of IHL to cyber operations: digital sovereignty, the classification of cyberattacks, and the distinction between military and civilian objectives in cyberspace. For the first time within a single analytical framework, it juxtaposes Russian and Western approaches to sovereignty in the digital domain, to the thresholds for qualifying cyber activities as "attacks," and to the legal status of data and dual-use objects for humanitarian protection purposes. The findings demonstrate that divergent national approaches to digital sovereignty and attribution impede the development of common criteria for applying the IHL principles of distinction, proportionality and precaution to cyber operations that do not involve physical destruction. The article therefore argues for clarifying the status of data as objects protected under IHL and for adapting traditional categories of military and civilian objectives to the operating conditions of critical information infrastructure.

Key words: information and communication technologies, information law, digital sovereignty, cyber warfare, international security, critical infrastructure, humanitarian protection, attribution of cyber incidents, civilian population, dual-use, legal regime of data

Conflicts of interest. The author declares no conflicts of interest.

For citation: Kozyulin, V.B. (2026). The applicability of international humanitarian law to cyber operations: A review of Russian and Western approaches. *Vestnik RUDN. International Relations*, 26(1), 62–76. https://doi.org/10.22363/2313-0660-2026-26-1-62-76; EDN: TCJXVU

Проблема применимости международного гуманитарного права к кибероперациям: обзор российского и западных подходов

В.Б. Козюлин

Дипломатическая академия МИД РФ, Москва, Российская Федерация

✉ v.kozyulin@dipacademy.ru

Аннотация. Актуальность темы исследования обусловлена тем, что кибероперации становятся неотъемлемым элементом современных вооруженных конфликтов, при этом применимость международного гуманитарного права (МГП) к цифровой среде остается дискуссионной. На практике это проявляется в отсутствии устоявшихся критериев, позволяющих однозначно отнести конкретное кибервоздействие к «нападению», «использованию силы» или к недружественным, но формально правомерным действиям. В условиях трансграничности информационно-коммуникационных технологий (ИКТ), анонимности действий и вовлечения негосударственных акторов отсутствует единый подход к квалификации кибердеяний и защите гражданской инфраструктуры, что затрудняет выработку согласованной международной реакции на киберинциденты. Дополнительную сложность создает то, что значительная часть кибероперация не приводит к физическому разрушению, а выражается в потере функциональности систем, что ставит под вопрос традиционные представления о насилии и ущербе в МГП. Методологически исследование опирается на сравнительно-правовой анализ официальных национальных позиций, документов ООН и специализированных доктринальных источников, а также на системное толкование норм МГП применительно к новым видам вооруженного противоборства. Используются методы юридико-догматического анализа, контент-анализ государственных доктрин и экспертных комментариев, а также элементы кейс-стади в части рассмотрения типичных киберинцидентов, включая операции против объектов критической инфраструктуры и информационных систем двойного назначения. Научная новизна исследования состоит в комплексном раскрытии трех узловых аспектов применения МГП к кибероперациям: цифрового суверенитета, квалификации кибератак и разграничения военных и гражданских целей в киберпространстве. Впервые в единой рамке сопоставлены российский и западные подходы к понятию суверенитета в цифровой среде, к порогам отнесения кибервоздействий к «нападению», а также к статусу данных и объектов двойного назначения в контексте гуманитарной защиты. Полученные результаты показывают, что разнородность национальных подходов к цифровому суверенитету создает препятствия для выработки согласованных критериев применения принципов различения, соразмерности и предосторожности к кибероперациям, не сопровождающимся физическим разрушением. Обоснована необходимость уточнения статуса данных как объектов защиты по МГП и адаптации традиционных категорий военных и гражданских целей к условиям функционирования критической информационной инфраструктуры.

Ключевые слова: информационно-коммуникационные технологии, информационное право, цифровой суверенитет, кибервойна, международная безопасность, критическая инфраструктура, гуманитарная защита, атрибуция киберинцидентов, гражданское население, двойное назначение, правовой режим данных

Заявление о конфликте интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: *Козюлин В.Б.* Проблема применимости международного гуманитарного права к кибероперациям: обзор российского и западных подходов // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2026. Т. 26, № 1. С. 62–76. https://doi.org/10.22363/2313-0660-2026-26-1-62-76; EDN: TCJXVU

Introduction

The consideration of applying international law norms, including international humanitarian law (IHL), to cyber operations within the framework of the United Nations has demonstrated that reaching consensus remains a challenging task. Western countries argue that existing international law, particularly

IHL, is sufficient for regulating interstate confrontation in the field of information and communication technologies (ICTs), while issues of cyberterrorism and cybercrime should be addressed within a distinct branch of international law (Schmitt, 2017a). Russia, in turn, advocates establishing a comprehensive international mechanism for regulating the application of international law in the ICT domain under the auspices of the United Nations, emphasizing the need to account for the specific characteristics of the digital environment, such as the potential anonymity of its participants' actions.[1]

Russia and China, along with several of their partner states and international organizations, take the view that many key rules of international humanitarian law are not, at present, applied in practice to cyber incidents and therefore require further clarification.[2]

The main objectives of this study are to examine the applicability of international humanitarian law to cyber operations in armed conflicts, as well as to analyze the possibilities of modifying existing international legal mechanisms to address issues arising in the field of cyber warfare, such as attribution, military necessity, and the distinction between military and civilian objects.

The research novelty lies in its comprehensive examination of the applicability of IHL to cyberspace operations, a relatively understudied area of legal scholarship and international relations. The paper presents a critical analysis of various national perspectives—in particular, those of Western countries and Russia—on the interpretation and application of IHL in cyberspace, identifies gaps in the existing legal framework, and suggests areas for further development in this area.

The study's methodological basis is based on the general scientific principles of systematicity, historicism, and an interdisciplinary approach, which consider cyber operations as an element of the evolution of armed conflicts and international legal regulation. This framework is supported by specialized legal analysis methods, such as a comparative legal analysis of national approaches to applying international humanitarian law in cyberspace, as well as a doctrinal analysis of relevant literature and international documents, which reveal discrepancies in the interpretation of digital sovereignty, cyberattacks, and the status of data.

Western School of Application of IHL to Cyber Operations

The fundamental document of Western legal scholarship on cyberspace regulation is the Tallinn Manual, developed under the guidance of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Centre of Excellence. The first edition (2013) focused on applying *jus ad bellum* and *jus in bello* to cyber operations, establishing criteria for qualifying a "cyberattack" as an act of violence (Schmitt, 2013). Even before the publication of the Tallinn Manual, N. Melzer, in a work prepared for the United Nations Institute for Disarmament Research (UNIDIR), identified the main conflicts in the application of *jus ad bellum* and *jus in bello* to cyberwarfare,

[1] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[2] Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/76/135 // The United Nations. July 14, 2021. (In Russian). URL: https://digitallibrary.un.org/record/3964709/files/DSS_33_Russian.pdf (accessed: 28.09.2025).

including issues of the threshold of armed conflict and attribution (Melzer, 2011).

In E.T. Jensen's article (Jensen, 2017) and in the publication *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, the author and a group of NATO experts elaborate on the applicability of *jus ad bellum* and *jus in bello* norms to cyber operations, proposing a framework of rules on issues of sovereignty, due diligence, the qualification of cyberattacks and the protection of civilian objects (Schmitt, 2017b).

Experts led by M. Schmitt developed a detailed system for applying current international law to cyber operations, including the principles of distinction, proportionality, and precaution (Schmitt, 2017b, pp. 54–68). The concept of "armed attack" was expanded to include highly destructive cyber operations and the relationship between *jus ad bellum* and *jus in bello* in the digital environment was clarified (Schmitt, 2017b). In a subsequent publication, M. Schmitt systematized the evolution of the jus ad bellum doctrine as applied to cyberspace over the past decade, stating that, despite growing consensus on a number of issues, the problem of the "threshold" for an armed attack remains unresolved (Schmitt & Pakkam, 2024).

M. Roscini's monograph analyzes the cases in which cyber operations can be considered a "use of force" or an "armed attack" within the context of the principles of the UN Charter and how the law of armed conflict regulates the choice of means and methods of cyberwarfare. The author examines in detail "borderline" scenarios where cyberattacks do not result in physical destruction but create significant functional consequences for critical infrastructure (Roscini, 2014, pp. 367–368).

The International Committee of the Red Cross (ICRC) is also actively developing the concept of protecting civilian objects in cyberspace.[3] The ICRC proposed the innovative idea of a "digital emblem" to protect medical and humanitarian organizations from cyberattacks.[4] One of the first systematic studies on this issue was the work of C. Droege, which substantiated the need to extend the principles of civilian protection to cyberspace operations and analyzed the limits of the applicability of jus in bello norms to cyberattacks that do not result in physical destruction (Droege, 2012).

Research by the ICRC's Legal Department plays a particularly important role in developing humanitarian perspectives. In their article, L. Gisel, T. Rodenhäuser, and K. Dörmann argue that cyber operations during armed conflicts clearly fall under IHL, while key issues include the criteria for classifying specific cyber actions as "attacks" and the question of whether data should be protected on an equal basis with civilian material objects (Gisel, Rodenhäuser & Dörmann, 2020).

The US Department of Defense emphasizes that the principles of the law of war apply to cyber operations regardless of the formal status of an armed conflict. In his statement, General Counsel P.S. Ney emphasizes that the consequences of cyber operations must be assessed based on their equivalence to the use of force by conventional means, and also establishes the obligation to observe the principles of distinction, proportionality, and precaution when planning and conducting military cyber

[3] International Humanitarian Law and Cyber Operations during Armed Conflicts // International Committee of the Red Cross. November 28, 2019. URL: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (accessed: 28.09.2025).

[4] Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems // International Committee of the Red Cross. November 3, 2022. URL: https://www.icrc.org/en/document/icrc-digital-emblems-report (accessed: 28.09.2025).

operations.[5] The American approach focuses on the outcome of an attack (functional damage, disruption of critical infrastructure) rather than the specific technical means, allowing existing IHL norms to be extended to a broad range of cyber activities.

The Netherlands, France, the United Kingdom and Australia recognize the applicability of IHL to cyberspace, with varying interpretations of the principles of sovereignty and non-interference.

In a 2019 parliamentary letter, the Netherlands presented a comprehensive position on the application of international law in cyberspace, explicitly recognizing sovereignty as an independent obligation, the violation of which through cyber operations may constitute an internationally wrongful act. The Dutch approach elaborates on the permissibility of countermeasures, attribution, and the political coordination of responses to cyberattacks, emphasizing that existing international law provides a sufficient basis for regulating state behavior in the digital environment.[6]

In its 2019 *Statement on International Law in Cyberspace*, France reaffirmed the applicability of the principles of sovereignty, non-intervention, and the prohibition of the threat of force to cyber operations and maintains that any cyberattack that violates the confidentiality, integrity, or availability of French information systems, when attributed to another state, constitutes, at a minimum, a violation of France's sovereignty. The French position emphasizes that the right to countermeasures and self-defense in cyberspace must be exercised strictly within the framework of international law, and that this excludes "retaliatory hacking actions" by private companies.[7]

In its 2021 official statement, the United Kingdom reaffirmed that international law fully applies to state activities in cyberspace, but adopted a more reserved position on sovereignty as an independent basis for responsibility, believing that the principle of sovereignty itself does not constitute a separate "prohibition" for cyber operations beyond the norms of non-interference.[8] Speeches by the Attorney General (J. Wright in 2018[9] and S. Braverman in 2022[10]) distinguish between cyber operations that reach the threshold of the use of force and armed attack, and other hostile, but smaller-scale, cyber activities.

Australia's policy document emphasizes that the UN Charter as a whole, including its provisions prohibiting the threat of force, self-defense, and state responsibility, is fully

[5] Ney Jr. P.C. DoD General Counsel Remarks at U.S. Cyber Command Legal Conference // U.S. Department of War. March 2, 2020. URL: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference (accessed: 28.09.2025).

[6] Schmitt M. The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis // Just Security. October 14, 2019. URL: https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/ (accessed: 28.03.2025).

[7] Roguski P. France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I // Opinio Juris. September 24, 2019. URL: https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed: 28.09.2025).

[8] Application of International Law to States' Conduct in Cyberspace: UK Statement // Foreign, Commonwealth & Development Office. June 3, 2021. URL: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (accessed: 28.09.2025).

[9] Speech: Cyber and International Law in the 21st Century // Gov.uk. May 23, 2018. URL: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed: 28.03.2025).

[10] Jowitt T. UK Can Legally Launch Cyberattacks Against Hostile Nations, Says AG // Silicon. May 19, 2022. URL: https://www.silicon.co.uk/e-regulation/governance/uk-legally-launch-cyberattacks-says-ag-458458 (accessed: 28.03.2025).

applicable to cyber operations, but also identifies new challenges related to sovereignty, attribution, and jurisdiction. Australia explicitly refers to the rules on international state responsibility and emphasizes the need for transparency in national interpretations of international law in cyberspace.[11]

Thus, an analysis of the positions of Western states and international organizations reveals that, despite broad agreement regarding the applicability of existing international law and IHL to cyber operations, differences persist regarding the content of digital sovereignty, the thresholds for classifying cyberattacks as "use of force" or "armed attack," and the procedures for international legal attribution. The issue of distinguishing between military and civilian targets in the digital environment also requires further study, including the legal regime for critical information infrastructure and data as potential objects of protection under IHL (Giovanelli, 2025).

Russian Studies

The Russian scholarly school is represented by the works of S.Y. Garkusha-Bozhko, who explores the issues of *ratione materiae* ("by virtue of the subject matter," "due to the essence of the matter") and *ratione temporis* ("by reason of time") in the application of IHL in cyberspace. The author highlights the significant difficulties in qualifying cyber operations as acts of armed conflict and emphasizes the need for a broader understanding of information warfare. S.Y. Garkusha-Bozhko demonstrates that the lack of a consistent understanding of "armed attack" and "cyberattack" leads to discrepancies regarding the legality of the use of force and humanitarian protection (Garkusha-Bozhko, 2021).

A.V. Korotkov and E.S. Zinovieva examine the security of critical information infrastructures in international humanitarian law, focusing on the challenges of distinguishing between military and civilian targets in the context of dual-use digital assets (Korotkov & Zinovieva, 2011).

Russia's official position is set out in the comments to the documents of the Open-Ended Working Group, emphasizing the need to take into account the sovereign rights of states in the information space.[12] Russian diplomacy operates in accordance with Decree No. 213 of the President of the Russian Federation dated April 12, 2021, which defines assistance in improving, under the auspices of the UN, the principles and norms of IHL as applied to the ICT sector.[13]

In the article *International Law and Warfare in Cyberspace*, G.G. Shinkaretskaya examines the applicability of IHL norms to attacks on information and cyber systems and concludes that the basic principles of IHL (distinction, proportionality, and precaution) fully apply in cyberspace. However, specific norms regarding cyber weapons and cyber operations are still being developed, creating legal uncertainty for states (Shinkaretskaya, 2013).

[11] 2017 — Australia's Position on the Application of the International Law to State Conduct in Cyberspace // Department of Foreign Affairs and Trade. URL: https://www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf (accessed: 01.02.2025).

[12] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[13] Decree of the President of the Russian Federation No. 213 "On Approval of the Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security" Dated April 12, 2021 // President of Russia. (In Russian). URL: http://www.kremlin.ru/acts/bank/46614 (accessed: 28.09.2025).

A more recent work, *Counteracting Cyberattacks: Gaps in International Law and Prospects for Overcoming Them*, analyzes the legal consequences of cyberattacks, the complexities of attribution and accountability, and national and international responses to cyber threats. The authors systematize existing international legal mechanisms for self-defense and collective security in the cybersphere and emphasize the need to develop special procedures and evidentiary standards for the international attribution of cyber incidents (Rahman & Das, 2024).

Digital Sovereignty in the Context of IHL

The concept of digital sovereignty implies the right of a state to control information flows within its territory and ensure the security of the national information space.[14] In the context of IHL, this concept takes on particular significance in determining jurisdiction and the law applicable to cyber operations.

The concept of "sovereignty" is evolving, and while it previously extended to airspace and the continental shelf, today the concept of "digital sovereignty" is emerging, which is a subset of technological sovereignty (sovereignty over data and digital infrastructure, including critical infrastructure).

Russia's Position on Digital Sovereignty

Russia consistently defends the principle of state information sovereignty.[15] The documents submitted to the Open-Ended Working Group emphasize "the sovereign right of each state to ensure the security of its national information space and to establish norms and mechanisms for managing its information and cultural space in accordance with national legislation."[16]

N.P. Romashkina defines information sovereignty as the state's ability to ensure the independence and constitutional rights of citizens in the information space.[17]

E.S. Zinovieva and S.V. Shitkov view digital sovereignty as a dynamic category, changing with the development of public policy and technology (Zinovieva & Shitkov, 2023). In the context of this discussion, the relationship between cybersecurity and sovereignty is attracting increasing attention: recent research documents growing competition among national models of digital sovereignty and the associated challenges to the international legal order (Lazari, 2025).

Russia advocates for the adoption of a convention on international information security under the auspices of the UN, which would take into account various aspects of the application of international law in the ICT sector.[18] To this end, Russian experts have developed a draft UN Convention *On Cooperation in Combating*

[14] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[15] Ibid.

[16] Ibid.

[17] Romashkina N.P. Information Sovereignty or Why Russia Needs an Information Security Strategy // Russian International Affairs Council. August 6, 2019. (In Russian). URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnyy-suverenitet-ili-pochemu-rossii-nuzhna-strategiya-informatsionnoy-bezopasnosti/ (accessed: 28.09.2025).

[18] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

Information Crime,[19] and, in 2023, proposed a *Concept for a UN Convention on International Information Security* for consideration.[20]

In the Russian doctrine, the need to form a comprehensive regime of international information security is substantiated in detail in a collective monograph edited by A.A. Streltsov, A.Ya. Kapustin, and others, which analyzes the military-political, legal, and technological dimensions of the use of ICT for the purposes of strategic deterrence and security (Streltsov et al., 2023).

Western Approaches to Digital Sovereignty

The positions of Western states vary in detail, but are united by a common approach to the application of current international law.

The United States expresses its position as follows. First, it confirms that the principle of territorial jurisdiction remains valid, even when applied to cyberattacks. Second, it emphasizes that the exercise of jurisdiction by a state within its territory is not absolute and must comply with international law, including international human rights obligations.[21] K. Bannelier-Christakis proposes the concept of "cyber diligence" as a minimum normative standard obliging states to prevent the use of their information infrastructure for cross-border cyberattacks (Bannelier-Christakis, 2014). A. Coco and T. de Souza Dias have demonstrated that the principle of due diligence in cyberspace remains patchwork and fragmented across various branches of international law, making it difficult to develop a unified regime of preventive state responsibility (Coco & de Souza Dias, 2021).

The main problem is the lack of clear criteria for determining territorial jurisdiction in cyberspace. M. Schmitt systematizes these "grey zones" of international cyberlaw, demonstrating that it is precisely the ambiguity of sovereignty and jurisdiction thresholds that allows states to act below the level of legal qualification, avoiding accountability (Schmitt, 2017a). Cyber operations can be conducted through servers located in different states, making it difficult to determine the applicable law (Giovanelli, 2025). The development of international standards for delineating jurisdictions and coordinating law enforcement practices is needed.

For its part, the ICRC launched a project to develop a digital emblem designed to "highlight" civilian assets online. In collaboration with the Center for Cyber Trust, Johns Hopkins University, and ITMO University in St. Petersburg, the ICRC developed technical solutions for identifying the digital infrastructure of protected organizations in cyberspace.[22]

[19] Draft United Nations Convention on Cooperation in Combating Cybercrime // Ministry of Foreign Affairs of the Russian Federation. January 19, 2018. (In Russian). URL: https://www.mid.ru/ru/foreign_policy/un/1561374/ (accessed: 28.09.2025).

[20] Updated Concept of the United Nations Convention on International Information Security // Security Council of the Russian Federation. May 16, 2023. (In Russian). URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (accessed: 28.09.2025).

[21] Official Compendium of Voluntary National Submissions on How International Law Applies to the Use of Information and Communication Technologies by States. A/76/136 // United Nations. July 13, 2021. (In Russian). URL: https://documents.un.org/doc/undoc/gen/n21/189/50/pdf/n2118950.pdf (accessed: 28.09.2025).

[22] The ICRC Proposes a Digital Red Cross/Red Crescent Emblem to Serve as a Sign of Protection in Cyberspace // International Committee of the Red Cross. November 3, 2022. (In Russian). URL: https://www.icrc.org/ru/document/mkkk-predlagaet-vvesti-cifrovuyu-emblemu-krasnogo-krestakrasnogo-polumesyaca-kotoraya (accessed: 28.09.2025).

Cyberattacks: Definition and Attribution of Responsibility

The Concept of "Cyberattack" in International Humanitarian Law

Based on Article 49 of Additional Protocol I, the Tallinn Manual 1.0 provided the following definition of a cyberattack: "A cyberattack is a cyber-operation, whether offensive or defensive, that can reasonably be expected to cause injury or death to persons or damage to or destruction of objects" (Schmitt, 2013, p. 106). This means that only those "military operations" that constitute an "act of violence" can be called "attacks" and, therefore, should be considered prohibited under IHL.

G.G. Shinkaretskaya points out that existing definitions of the term "cyberattack" do not take into account the specific features of cyberattacks that do not result in physical damage, and she justifies the need to develop an independent definition of a cyberattack that reflects the specifics of the digital environment (Shinkaretskaya, 2023). However, cyber operations are generally not "violent," which presents a problem when applying IHL to them. As for the term "military action," its use in relation to cyber operations may require amendments to IHL.

According to the position adopted by the International Committee of the Red Cross, any operation during an armed conflict aimed at disrupting the functioning of a computer or computer network is qualified as an attack under the definition of international humanitarian law, regardless of the method of disabling the object — whether physical destruction or other methods of influence.[23]

According to Y.M. Haminskiy, a Russian legal expert, one of the key challenges associated with cyberspace is the need to resolve the question of whether certain tools and methods of cyberwarfare should be completely banned or regulated by international agreements (Haminskiy, 2021).

Given new technological developments, many experts believe that the concept of "violence" must be expanded to include, in addition to "material damage to objects," "disabling infrastructure without destruction" (Roscini, 2014, p. 181; Gisel, Rodenhäuser & Dörmann, 2020). A similar position is taken by H. Lin, who points out that the classical IHL categories of "attack," "means of warfare," and "military necessity" — when interpreted literally — do not cover a significant portion of cyber actions, and proposes a functional approach to their classification (Lin, 2012).

R. Buchan and N. Tsagourias further raise the question of command responsibility for the use of autonomous cyber capabilities, demonstrating that the automation of attacks complicates not only attribution, but also compliance with the principles of distinction and proportionality (Buchan & Tsagourias, 2020).

It appears appropriate to extend IHL norms to non-destructive cyber operations, including the disabling of military systems, interference with information networks, intelligence operations, temporary infrastructure disruption, and psychological operations.

Problems of Attribution of Responsibility in Cyberspace

Currently, the attribution of responsibility is a complex problem due to the potential for attacking states to exploit the territories of third countries and proxy actors. N. Tsagourias was one of the first to demonstrate that the anonymity

[23] International Humanitarian Law and Cyber Operations during Armed Conflicts // International Committee of the Red Cross. November 28, 2019. URL: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (accessed: 28.09.2025).

and cross-border nature of cyberattacks undermine traditional mechanisms for attributing responsibility for these attacks and call into question the right to self-defense provided for in Article 51 of the UN Charter (Tsagourias, 2012).

Currently, international legal attribution is speculative and subjective in nature, and it can be used to achieve one's own political objectives or as an information warfare tool to undermine the image of a strategic adversary (Romashkina, Markov & Stefanovich, 2020). Unified mechanisms for disclosing attribution methodology and providing a comprehensive evidence base to the international community are lacking. N. Tsagourias and M. Farrell emphasize that the gap between the technical and legal standards of attribution remains a key obstacle to the development of an international cyber liability regime (Tsagourias & Farrell, 2020).

According to Russian analysts, the influence of non-state and non-governmental actors in the information sphere has reached a level comparable to state power (Korotkov & Zinovieva, 2011). According to the official Russian position, any accusations against states of organizing and committing illegal actions must be substantiated, and publicly attributing responsibility for incidents in the information space to a specific state is unacceptable without the presentation of relevant technical evidence.[24]

The US leadership, on the contrary, believes that there is no international legal obligation to disclose the evidence on which the attribution of a cyberattack is based. Therefore, a state does not require absolute certainty, as it acts as its own judge and can make a unilateral decision regarding the attribution of a cyberoperation to another state.[25] K. Eichensehr analyzes in detail the political and legal logic of this position, demonstrating that, in US practice, attribution serves both as an expansion of executive authority and as a deterrent, while the standard of proof remains below the judicial threshold (Eichensehr, 2020).

UN General Assembly (UNGA) Resolution 70/237 calls on states to cooperate in sharing information and bringing to justice those involved in the criminal use of ICTs. On December 24, 2024, the UNGA session unanimously supported the Russian-proposed *Convention against Cybercrime; Strengthening International Cooperation to Combat Certain Crimes Committed through the Use of Information and Communications Systems and in the Exchange of Electronic Evidence Relating to Serious Crimes*.[26]

D.D. Shtodina characterizes the adoption of this Convention as the result of a "cyber compromise," in which the contradictions between Western and non-Western approaches were resolved at the expense of a framework

[24] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[25] See, e.g.: Eichensehr K. Cyberattack Attribution and International Law // Just Security. July 24, 2020. URL: https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/ (accessed: 05.03.2026). The author, summarizing the practice and statements of the United States, notes that, despite the proposals of some states, "there is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action."

[26] Convention against Cybercrime; Strengthening International Cooperation to Combat Certain Offences Committed through Information and Communications Systems and in the Exchange of Evidence in Electronic Form Relating to Serious Crimes // United Nations. December 24., 2024. (In Russian). URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (accessed: 28.09.2025).

of wording with considerable room for national interpretation (Shtodina, 2025).

Thus, the trend toward the development of special treaty mechanisms for the exchange of technical and evidentiary information on cyber incidents is being consolidated at the universal level, which could potentially contribute to the development of more transparent procedures for international legal attribution and the strengthening of trust between states in the ICT sector.

Distinction between Military and Civilian Targets in Cyberspace

The distinction between military and civilian targets in cyberspace is complicated by the dual purpose of digital assets. In its approach to cyber operations, Washington emphasizes that, even if the rules of the law of war are not formally applied because the proposed military cyber operation is conducted outside the context of an armed conflict, the Department of Defense still adheres to the principles of the law of war.[27]

The Tallinn Manual 2.0 establishes that civilian objects in cyberspace are protected from direct attacks (Schmitt, 2017b).

Russia warns against attempts to "impose the principle of the full and automatic applicability of international humanitarian law to the information and communications environment in peacetime."[28] Russian experts note that humanitarian critical information infrastructure facilities lack any special distinguishing features confirming their special legal status, and in the context of information warfare, it is extremely difficult to clearly distinguish between civilian and military targets (Korotkov & Zinovieva, 2011; Adu & Ramich, 2025).

The Russian position is that "the information environment possesses unique technical and legal characteristics that preclude the automatic and full application of current international law. This applies, in particular, to such features as the transborder and pervasive nature of ICTs, the anonymity of their use and the difficulty of reliably identifying the source of malicious activity, the possibility of introducing hidden malicious functions and software and hardware vulnerabilities, and the permissibility of using ICTs for dual-use purposes."[29]

Therefore, the existing definitions of military and civilian objects in IHL require clarification, given that military systems operate on the basis of civilian infrastructure.

Protection of Critical Infrastructure

Protecting critical information infrastructure poses a particular challenge. Power, water, transportation, and communications systems are primarily civilian assets, but they can make an effective contribution to military action.[30]

[27] Ney Jr. P.C. DoD General Counsel Remarks at U.S. Cyber Command Legal Conference // U.S. Department of War. March 2, 2020. URL: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference (accessed: 28.09.2025).

[28] Commentary of the Russian Federation on the Initial Pre-draft of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security // UN Office for Disarmament Affairs. April 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf (accessed: 28.09.2025).

[29] Statement by I.A. Tyazhlova, Representative of the Russian Federation, at the Seventh Session of the UN Open-Ended Working Group on Security in the Use of ICTs and ICTs Themselves, 2021–2025, under the Agenda Item "How International Law Applies to the Use of ICTs by States" // Permanent Mission of the Russian Federation to the UN. March 6, 2024. (In Russian). URL: https://russiaun.ru/ru/news/060324 (accessed: 29.09.2025).

[30] Roguski P. France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I // Opinio Juris. September 24, 2019. URL: https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed: 28.09.2025).

Danish[31] and Norwegian military guidelines[32] provide for the possibility of attacks on dual-use facilities, subject to the principle of proportionality.

According to the ICRC, information related to medical facilities, humanitarian organizations, and civilian life support systems, such as water treatment plants and irrigation systems, are subject to special protection under international humanitarian law. As part of the development of the "digital emblem," the ICRC intends to use it to protect medical facilities in cyberspace.[33]

Protecting citizens' personal data from malicious cyber activity in armed conflicts is becoming an increasingly important task.

However, the status of data as an object of protection under IHL remains controversial. Most experts drafting the Tallinn Manual concluded that data per se are not objects within the meaning of Article 52 of Additional Protocol I (Schmitt, 2017b).

According to the position of the Danish Ministry of Defence, digital data are generally not classified as an object.[34]

In contrast, the Norwegian Defence Ministry is of the opinion that data should be classified as objects and that direct attacks on them are only permissible in cases where they constitute a legitimate military target.[35]

According to the French side, various types of information content (including civil, banking and medical data) are protected in accordance with the principle of distinction between civilian and military objects.[36]

This approach has been criticized by Russian experts, who point to the potential for causing significant harm to civilians through data attacks without physical damage to infrastructure (Garkusha-Bozhko, 2021). Further consideration of the legal status of data in the context of protecting civilian objects is required.

It appears that, in the context of the growing digital interdependence of society, ignoring data as an independent object of protection effectively erodes the humanitarian guarantees enshrined in IHL. The Danish position, assuming that digital data are "generally" not considered an object, reflects a cautious but, in the long term, insufficient approach, as it fails to adequately consider the consequences of cyber operations targeting information assets on which the lives and health of the civilian population depend. The Norwegian and French approaches, by contrast, appear more consistent with the humanitarian objective of IHL, as they explicitly recognize the need to consider the impact on data within the context of an armed conflict and link the permissibility of attacks to the criterion of a legitimate military

[31] Military Manual for the Danish Defence // The Danish Armed Forces. October 12, 2020. URL: https://www.forsvaret.dk/en/publications/military-manual/ (accessed: 28.09.2025).

[32] Manual i krigens folkerett. Oslo : Forsvarssjefen, 2013 // Databases on International Humanitarian Law. URL: https://ihl-databases.icrc.org/ru/national-practice/manual-i-krigens-folkerett?activeTab=all-national-practice (accessed: 28.09.2025).

[33] Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks and Possible Solutions. International Committee of the Red Cross, 3 November 2022. URL: https://www.icrc.org/en/document/icrc-digital-emblems-report (accessed: 28.09.2025).

[34] Military Manual for the Danish Defence // The Danish Armed Forces. October 12, 2020. URL: https://www.forsvaret.dk/en/publications/military-manual/ (accessed: 28.09.2025).

[35] Manual i krigens folkerett. Oslo : Forsvarssjefen, 2013 // Databases on International Humanitarian Law. URL: https://ihl-databases.icrc.org/ru/national-practice/manual-i-krigens-folkerett?activeTab=all-national-practice (accessed: 28.09.2025).

[36] Roguski P. France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I // Opinio Juris. September 24, 2019. URL: https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed: 28.09.2025).

objective and the principle of distinction. In this regard, the most justified option seems to be the evolutionary development of IHL in the direction of recognizing at least certain categories of data (medical, humanitarian, critical for life support) as objects enjoying special protection, with the subsequent development of clear criteria for classifying them as civilian or military targets and the corresponding adaptation of the rules of proportionality and precaution.

Conclusion

An analysis of three key aspects of the application of IHL to cyber operations reveals significant gaps in international legal regulation in this area.

First, within the discussion of digital sovereignty, there is no international consensus regarding the scope of states' sovereign rights in cyberspace. Russia's approach to information sovereignty is not sufficiently reflected in Western concepts of IHL application. The development of international standards for delineating jurisdictions and coordinating law enforcement practices is needed.

Second, existing definitions of cyberattacks do not take into account the specifics of information-psychological influence. Attribution issues require the development of new international mechanisms for investigating cyber incidents with uniform standards of evidence.

Finally, the principle of distinguishing the targets of cyberattacks requires adaptation to the conditions of the digital environment. The legal status of data and the criteria for protecting dual-use assets need to be clarified.

Further research in this area should focus on developing specific mechanisms for implementing IHL in cyberspace and studying state practices in responding to cyber threats within the context of international humanitarian law. Only synchronization of legal, technological, and political aspects will allow the creation of a sustainable system for regulating digital conflicts.

Received / Поступила в редакцию: 20.06.2023
Revised / Доработана после рецензирования: 13.11.2025
Accepted / Принята к публикации: 18.12.2025

References

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; EDN: KACFAB

Bannelier-Christakis, K. (2014). Cyber diligence: A low-intensity due diligence principle for low-intensity cyber operations? *Baltic Yearbook of International Law*, 14(1), 23–39. https://doi.org/10.1163/22115897-90000118

Buchan, R., & Tsagourias, N. (2020). Autonomous cyber weapons and command responsibility. *International Law Studies*, 96, 645–673. Retrieved from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2935&context=ils

Coco, A., & de Souza Dias, T. (2021). "Cyber due diligence": A patchwork of protective obligations in international law. *European Journal of International Law*, 32(3), 771–806. https://doi.org/10.1093/ejil/chab056; EDN: ODWVJK

Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 94(886), 533–578. https://doi.org/10.1017/S1816383113000246

Eichensehr, K.E. (2020). The law and politics of cyberattack attribution. *UCLA Law Review*, 67(3), 520–598. Retrieved from https://www.uclalawreview.org/wp-content/uploads/securepdfs/2020/09/Eichensehr-67-3.pdf

Garkusha-Bozhko, S.Y. (2021). International humanitarian law in cyberspace: Ratione materiae, ratione temporis and problem of cyber-attack qualification. *Digital Law Journal*, 2(1), 64–82. (In Russian). https://doi.org/10.38044/2686-9136-2021-2-1-64-82; EDN: UKFVGJ

Giovanelli, D. (2025). Handling cyberspace's state of intermediacy through existing international law. *International Review of the Red Cross*, 107(928), 96–139. https://doi.org/10.1017/S1816383124000390; EDN: GFPZVF

Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, 102(913), 287–334. https://doi.org/10.1017/S1816383120000387; EDN: ZLBTAJ

Haminskiy, Y.M. (2021). The role of international humanitarian law in the era of cyber threats. *Advances in Law Studies*, (1), 56–60. (In Russian). https://doi.org/10.29039/2409-5087-2021-9-1-56-60; EDN: FEWNTC

Jensen, E.T. (2017). The Tallinn Manual 2.0: Highlights and insights. *Georgetown International Law Journal*, 48(3), 735–778. Retrieved from https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

Korotkov, A.V., & Zinovieva, E.S. (2011). Security of critical information infrastructures in international humanitarian law. *MGIMO Review of International Relations*, (4), 154–162. (In Russian). EDN: OOQRAD

Lazari, S.S. (2025). Cybersecurity and sovereignty in cyberspace: Challenges and prospects of international law. *Moscow Journal of International Law*, (1), 125–137. (In Russian). https://doi.org/10.24833/0869-0049-2025-1-125-137; EDN: HLNRTE

Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross*, 94(886), 515–531. https://doi.org/10.1017/S1816383112000811

Melzer, N. (2011). *Cyberwarfare and international law*. Geneva: UNIDIR. Retrieved from https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf

Rahman, M.M., & Das, T.K. (2024). Countering cyberattacks: Gaps in international law and prospects for overcoming them. *Journal of Digital Technologies and Law*, 2(4), 973–1002. https://doi.org/10.21202/jdtl.2024.46; EDN: NNFTQI

Romashkina, N.P., Markov, A.S., & Stefanovich, D.V. (2020). *International security, strategic stability and information technologies*. Moscow: IMEMO RAN publ. (In Russian). https://doi.org/10.20542/978-5-9535-0581-9; EDN: NYGUJH

Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199655014.001.0001

Schmitt, M.N. (2013). *Tallinn Manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, M.N. (2017a). Grey zones in the international law of cyberspace. *Yale Journal of International Law Online*, 42(2), 1–21. Retrieved from https://bpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf

Schmitt, M.N. (2017b). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

Schmitt, M.N., & Pakkam, A.S. (2024). Cyberspace and the jus ad bellum: The state of play. *International Law Studies*, 103, 194–229. Retrieved from https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3085&context=ils

Shinkaretskaya, G.G. (2013). International law and war in the cyberspace. *Sovremennoe Pravo*, (8), 120–126. (In Russian). EDN: QZLCUF

Shinkaretskaya, G.G. (2023). The problem of defining a cyber attack. *International Law*, (2), 10–21. (In Russian). https://doi.org/10.25136/2644-5514.2023.2.40051; EDN: NYDJJZ

Shtodina, D.D. (2025). United Nations Convention against Cybercrime, 2024 — the outcome of "cyber compromise"? *Moscow Journal of International Law*, (1), 110–124. (In Russian). https://doi.org/10.24833/0869-0049-2025-1-110-124; EDN: XIIYBP

Streltsov, A.A., Kapustin, A.Ya., Polyakova, T.A., Markov, A.S., & Miroshnikov, B.N. (Eds.). (2023). *International security in the environment of information and communication technologies*. Moscow: NAMIB publ. (In Russian). EDN: FBKNHG

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, 17(2), 229–244. https://doi.org/10.1093/jcsl/krs019

Tsagourias, N., & Farrell, M. (2020). Cyber attribution: Technical and legal approaches and challenges. *European Journal of International Law*, 31(3), 941–967. https://doi.org/10.1093/ejil/chaa057; EDN: JKNLRK

Zinovieva, E.S., & Shitkov, S.V. (2023). Digital sovereignty in the practice of international relations. *Mezhunarodnaa Zizn'*, (3), 38–51. (In Russian). EDN: HBTQYT

About the author:

Kozyulin Vadim Borisovich — PhD (Political Sciences), Chief Research Fellow, Center for Military-Political Studies, Institute of Contemporary International Studies; Associate Professor at the Department of Public Administration, Diplomatic Academy of the Ministry of Foreign Affairs of Russia; 153/2 Ostozhenka St, Moscow, 119021, Russian Federation; eLibrary SPIN-code: 6736-6554; ORCID: 0000-0001-6705-5303; e-mail: v.kozyulin@dipacademy.ru